Hidden Internet topologies info: Truth or Myth?

Sofía Silva Berenguer*, Esteban Carisimo†, J. Ignacio Alvarez-Hamelin†
and Francisco Valera Pintor*
* UC3M, Madrid, Spain. {ssilva,fvalera}@it.uc3m.es
† INTECIN (UBA-CONICET), Buenos Aires, Argentina. {carisimo,ihameli}@cnet.fi.uba.ar

ABSTRACT

Internet mapping projects usually get information from several routing data collectors or vantage points. The accuracy of maps relies on the amount and location of these collectors, which are usually near the backbone or at large developed regions, such as ARIN's or RIPE NCC's. The lack of vantage points in Latin America makes these maps not really show the current actual status of the network in this region. For this reason, in this work we have added data from some local sources and measured how much information was missing without them.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Network topology*

Keywords

Latin America, Network topology, traceroute

1 Introduction

The AS-level Internet topology has been widely studied for years using many different methodologies. The earliest studies about the Internet AS-level topology [6, 10] are from between 1997 and 1999. For this kind of studies, the amount and location of the vantage points is crucial. A low number of vantage points in some regions may lead to the representation of a topology for that region being incomplete. This is probably one of the reasons behind the fact that most of the known studies have a world-wide scope and not a regional scope. An example of a regional study is [7], which evaluates the topology interconnecting ISPs based on Africa. But unfortunately, there are not many other examples of regional studies.

LANCOMM, August 22-26, 2016, Florianopolis , Brazil
 ISBN 978-1-4503-4426-5/16/08…$15.00
DOI: http://dx.doi.org/10.1145/2940116.2940118

On the other hand, it has been proven that a considerable amount (at least 35 %) of the links between ASes are not being discovered and that most of them are peer-to-peer links [8]. The reason for this is that peering relationships are usually not announced to transit providers or other peers, and therefore, a vantage point needs to be located at one of the peering ASes or at one of the peers' customer cones [9] in order to be able to discover the peering link. The inevitable consequence of this is that the Internet topology maps that can be created are incomplete, mostly for those regions where the number of vantage points is low (e.g., Africa and Latin America).

According to [3], AS maps can be enhanced by adding local routing information from Looking Glasses (LGs) and routing policy information from Internet Routing Registry (IRR) databases. The main purpose of this work is to add local routing information and measure the improvement accomplished.
For this article, we generate the typical Internet graphs representing the Autonomous Systems (ASes) as vertices and their corresponding relationships as edges. With the aim of analysing the impact on these graphs of adding local routing information to the publicly available routing information, we create graphs at three different levels of scope: country, region and world. Finally, we measure the enhancement on the graphs when adding local routing information.

2 Methodology

The graphs used as a reference point when making the comparisons are built from the BGP information offered by the RIPE RIS and RouteViews projects. The local routing information added in order to enhance the topology diagrams is BGP data obtained from different Looking Glasses in the Latin America and the Caribbean (LAC) region (CABASE (Argentina), PTT Metro (Brazil), etc.) and from *show ip bgp* outputs provided by some operators in the region. The lack of vantage points in Latin America has led to some projects, such as PladMeD [2], to develop their own platform to gather data from this region. PladMeD, which is a traceroute-based platform to study the

	$\|V\|$	$\|E\|$	$< d >$	$\max(d)$	$< cc >$	$< k >$	$\max(k)$
BO	17	17	2	6	0	1.2	2
BO+	19	32	3.37	8	0.44	2.2	3
LAC	4835	23056	9.54	811	0.42	4.8	27
LAC+	4926	30824	12.52	865	0.65	4.9	40
World	52688	204462	7.8	4777	0.27	3.9	75
World+	54270	222561	8.2	5133	0.30	4.2	76

Table 1: Analysed parameters for different scales, and their enhanced versions (plus sign).

improvements of the first Bolivian IXP, provides us detailed information about Bolivian ASes ecosystem. For the graphs at the country level, Bolivia is used as a case of study and apart from adding to the national graph the local routing information mentioned above, we also added relationships inferred from an AS paths' set from PladMed.

Relationships between ASes are inferred using CAIDA's AS Relationship inference algorithm [5]. Although the main focus of this algorithm is to identify the type of relationship between the ASes (Transit or Peering), the type of relationship is not used for this work, just the fact that a relationship between two ASes exists.

It is important to note that mainly two different criteria can be used to restrict an Internet topology graph to a certain area: 1) use the information of the country where the organisation to which the AS was assigned is based; 2) use geolocation information in order to determine the countries in which an AS is active, i.e., the countries to which the prefixes being announced by an AS are geolocated. Taking into account that an AS is not necessarily used in the country to which it was assigned, the first option is not used. Instead, the prefixes announced by all the active ASes were geolocated using RIPEstat Data API in order to determine the countries where each AS is active. To create the national graphs for Bolivia and the regional graphs for the LAC region, we filtered the World graphs in order to include just the ASes that are active in the area of interest and the relationships in which these ASes are involved.

Geolocation tools determinate which foreign ASes operate in Latin America and which Latin American ASes operate abroad. However, Latin American ASes rarely operate overseas or even in ARIN's region. In our study, inaccuracies could be at country-level graph with ASes that operate in several Latin American countries.

Although criterion 2) is more accurate than 1), there are some misleading entries on every geolocation database. In this case, RIPEstat shows that AS701, AS1239 and AS10434 are active in Bolivia but no dataset has shown a link between these ASes and other ASes truly participant in the Bolivian network. Due to this mistake, Bolivian graphs are not completely connected.

Looking for comparing the graphs we used the following parameters: $|V|$ (number of vertices), $|E|$ (number of edges), $< d >$ (average degree), $\max(d)$ (maximum degree), $< cc >$ (average clustering coefficient), $< k >$ (average shell index) and $\max(k)$ (maximum k-core). The average degree is computed as $< d >= \frac{2|E|}{|V|}$ and it measures the number of relationships in which an AS is involved on average. The average clustering coefficient as $\frac{1}{|V|}\sum_{1\leq i\leq|V|} cc(i)$, where $cc(i) = \frac{m(i)}{d(i)(d(i)-1)}$ is the clustering coefficient of vertex i, $d(i)$ is the degree of vertex i and $m(i)$ is the number of edges between the neighbours of i. The cc measures the level of interconnection within a node's neighbourhood. The k-core is a subgraph where all vertices have at least degree k. The k-shell-index is the maximum core a vertex belongs to. We use LaNet-vi [1] to compute the k-core decomposition (i.e, the computation of vertices belonging to each shell), and also to verify which vertices (or ASes in this case) verify the core-connectivity property.

3 Analysis

In order to study the improvement on the graphs introduced by the added Latin American vantage points, we analyse the changes on the three levels: *BO* is the Bolivian network, *LAC* is the Latin American network, *World* is the whole Internet. For each of them, we have the initial version (RIPE RIS and RouteViews) and the enhanced one (adding Looking Glasses and vantage points) distinguished with a plus sign. Table 1 displays the measured parameters for each graph. In this particular case, the six graphs show the *core-connectivity* [1] property, that is, a vertex in a k-core has at least k different paths to another vertex in the same k-core. This property was expected because the world ASes graphs have always verified this along the time. Therefore, a network with a large maximum k-core (or large $< k >$, the average shell-index) implies robustness because there are more paths to interconnect its ASes. We created a website [1] where the graphs generated by LaNet-vi are shown.

Regarding Table 1, we can affirm that when adding more local information about interconnection between ASes, the observed parameters increase. For instance, the average degree increases by 68% in *BO*, by 32% in LAC and by just 6% in World. Similar results have been found for the maximum degree: 33%, 6% and 7% respectively; clustering coefficient: *exists*, 23% and 9%

[1] http://cnet.fi.uba.ar/ASes_topology_LatAm/

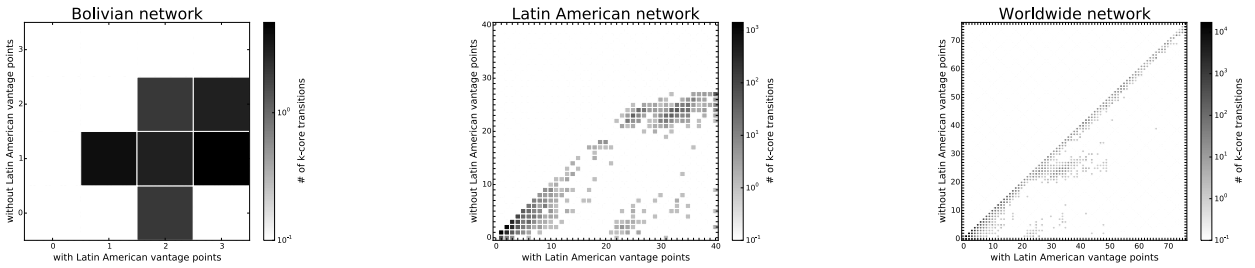


Figure 1: Improvement of k-shell-index sets (connectivity).

respectively; average shell-index (connectivity): 83%, 2% and 8% respectively; and finally maximum k-core: 50%, 48% and 1% respectively. This shows that the increment in the interconnection that was detected has a great impact on the national networks as *BO*, some impact on the regional ones as *LAC*, and less impact on the whole Internet. Moreover, the robustness detected, measured by the average shell-index $< k >$ (all graphs are core-connected, i.e., there are at least k different paths between ASes in a k-core subgraph) and the maximum k-core (the backbone of such network), has a great impact in national and regional networks, and much less in the World case.

Figure 1 shows the probability an AS has of changing from shell k to shell k' (the darker, the more probable) for the *BO*, *LAC* and *World* graphs. We observed that shells maintain or increase their value (i.e., $k' \geq k$), which is expected since new edges were added. The greatest impact is at the national and regional levels (*BO* and *LAC* networks), which is an expected result as we added national and regional routing information. It can also be noticed that the improvement at these levels has an impact on the *World* network (the reasons for which the *LAC* graph is improved also apply to the *World* graph as the first one is a subset of the latter). Moreover, this figure highlights the improvements are in the low and high shells for the *LAC* case, and the whole *BO* network. The impact on the *World* network shows the relative importance of the LAC region in the World network.

4 Conclusions

As suggested by [4], it seems that adding local routing information is highly relevant. For this reason, we wanted to verify if there is actually hidden information in regular Internet graphs. We have effectlively found that there is, as it is shown by the variation of the different computed metrics. We have also verified that the regional hidden information has a global impact, although a deeper analysis of the implications of the different metrics should be carried out as further study.

Acknowledgements. This work was partially founded by UBACyT 2014 (20020130200122BA). E.C. acknowledges CONICET Argentina for a PhD fellowship.

5 References

[1] M. G. Beiró, J. I. Alvarez-Hamelin, and J. R. Busch. A low complexity visualization tool that helps to perform complex systems analysis. *New J. Phys*, 10(12):125003, 2008.

[2] E. Carisimo, H. Galperin, and J. I. Alvarez-Hamelin. A new intrinsic way to measure ixp performance: an experience in bolivia. *arXiv e-print*, abs/1505.00837, May 2015.

[3] H. Chang, R. Govindan, S. Jamin, S. J. Shenker, and W. Willinger. Towards Capturing Representative AS-level Internet Topologies. *Comput. Netw.*, 44(6):737–755, Apr. 2004.

[4] L. Dall'Asta, J. I. Alvarez-Hamelin, A. Barrat, A. Vázquez, and A. Vespignani. Exploring networks with traceroute-like probes: Theory and simulations. *Theor. Comput. Sci.*, 355(1):6–24, 2006.

[5] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, G. Riley, et al. As relationships: Inference and validation. *SIGCOMM Comput. Commun. Rev.*, 37(1):29–40, 2007.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. *SIGCOMM Comput. Commun. Rev.*, 29(4):251–262, Aug. 1999.

[7] R. Fanou, P. Francois, and E. Aben. *PAM 2015, New York, NY, USA*, chapter On the Diversity of Interdomain Routing in Africa, pages 41–54. Springer International Publishing, Cham, 2015.

[8] 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.*, 17(2):391–404, Apr. 2009.

[9] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy. As relationships, customer cones, and validation. In *IMC 2013, Proceedings*, IMC '13, pages 243–256, New York, NY, USA, 2013. ACM.

[10] D. Magoni and J. J. Pansiot. Analysis of the autonomous system network topology. *SIGCOMM Comput. Commun. Rev.*, 31(3):26–37, July 2001.

Studying the Evolution of Content Providers in the Internet Core

Esteban Carisimo[†§*], Carlos Selmo[‡], J. Ignacio Alvarez-Hamelin[†‡*] and Amogh Dhamdhere[§]
† Universidad de Buenos Aires, ‡ Instituto Tecnológico de Buenos Aires, § CAIDA/UC San Diego, * CONICET
{carisimo,ihameli}@cnet.fi.uba.ar, cselmo@itba.edu.ar, amogh@caida.org

***Abstract*—There is recent evidence that the core of the Internet, which was formerly dominated by large transit providers, has been reshaped after the transition to a multimedia-oriented network, first by general-purpose CDNs and now by private CDNs. In this work we use *k*-cores, an element of graph theory, to define which ASes compose the core of the Internet and to track the evolution of the core since 1999. Specifically, we investigate whether large players in the Internet content and CDN ecosystem belong to the core and, if so, since when. We further investigate regional differences in the evolution of large content providers. Finally, we show that the core of the Internet has incorporated an increasing number of content ASes in recent years. To enable reproducibility of this work, we provide a website to allow interactive analysis of our datasets to detect, for example, "up and coming" ASes using customized queries.**

I. Introduction

The structure of the Autonomous System (AS) network has been changing over the years driven by disruptive changes on the Internet [1]. In the NSFNET era, the Internet had a monolithic backbone deployed in the U.S. to interconnect research and educational institutions [2]. After the US government decommissioned the NSFNET, the interdomain network moved onto a Transit era where the network had a hierarchical structure [1], [3]. More recently, the Internet has transformed into multimedia network, driven by high bandwidth demands and low latency requirements, resulting in a Content era [4].

Content Delivery Networks (CDNs) have played a decisive role in the evolution towards a multimedia network [5] and the resulting *flattening* of the Internet [1], [6]. CDNs are decentralized serving infrastructures that provide front-ends close to users to reduce latency, maximize the throughput and avoid delivering packets through long routes, which increase latency and can be congested [7]. CDNs typically establish a large number of peering agreements with ASes hosting customers of their content ("eyeballs"). It is not necessary that every Content Provider (CP) needs to deploy its own CDN. A number of *third-party CDNs* provide hosting services without being content generators, such as Akamai and LimeLight. However, it is apparent that several CPs have transformed into private CDNs with worldwide coverage instead of delivering content through Transit Providers or third-party CDNs due to a range of technical, economic, and legal reasons [8]–[13].

In addition to CDNs, Internet Exchange Points (IXPs) have been crucial in morphing the hierarchical structure of the AS internetwork, transforming it into a *flat* network [14]. The availability of IXPs is critical to CDNs, which prefer to have direct peering relationships with as many ASes as they can [15]. IXPs too are interested in hosting CDNs to provide a cost-effective way for the IXP members to reach content [16].

In this paper we use the term "core" of the network to refer to the subset of ASes that are densely connected. In the past the "core" of the network mostly consisted of tier-1 networks, which were large international transit providers that were connected to all other tier-1 networks with peering links and had no transit providers of their own. CPs, as well as "eyeball" networks that were the destinations of traffic sourced by CPs were on the edge of the network. However, CPs and third-party CDNs have been building intercontinental backbone networks as well as making thousands of peering agreements in recent years. The growing significance of CPs has led to discussion and speculation about whether CPs are now the dominant players in the Internet ecosystem [4].

Our goal is to investigate what role CPs now play in the Internet ecosystem, and in particular, if CPs are now a part of the "core" of the Internet. Specifically, we motivate this work with the following questions: How can we identify if a CP does or does not belong to the core of the Internet? If the core of the network does indeed include CPs, who are they? As the AS ecosystem has shown striking differences according to geographical regions [15], do we also see geographical differences in the role of CPs and their presence in the "core" of regional Internet structures? Finally, as more CPs deploy their private CDNs, can we detect "up and coming" CDNs that are not currently in the core of the network but are likely to be in the future?

We use the concept of *k-cores* to analyze the structure of the AS-level internetwork over the last two decades. We first focus on seven large CPs, and confirm that they are all currently in the core of the Internet. We then dig deeper into the evolution of these large players to correlate observed topological characteristics with documented business practices which can explain when and why these networks entered the core. We then take a broader view, characterizing the set of ASes in the core of the Internet in terms of business type and geography. Our analysis reveals that an increasing number of CPs are now in the core of the Internet. Finally, we demonstrate that the k-core analysis has the potential to reveal the rise of "up and coming" CPs. To encourage reproducibility of our results, we make our datasets available via an interactive query system at http://cnet.fi.uba.ar/TMA2018/.

II. Related work

The increasing importance of CDNs in the Internet ecosystem has produced a vast literature on this topic, which shares some of the goals of the present article. Several articles studied the internal structure of CDNs [17]–[20], where the focus was on the economic and technical benefits of CDNs, the need of data replication, techniques for content distribution and cache updates, and cache placement. CDN literature has also acknowledged the rising importance of private CDNs. Indeed, there have been several studies about the largest private CDNs. Google's CDN has been studied from many points of view: the growth of the serving infrastructure in recent years [21], QoE performance [22], internal load balancing [10], traffic engineering strategy run by its WAN SDN [9] and so on. Facebook's CDN was studied from the point of view of data replication [23], network administration [24], and Facebook's SDN [11]. Bottger et al. [25] studied the Netflix serving infrastructure, called Open Connect, due to its remarkably different architecture from other CDNs as well as the importance of Netflix in overall traffic share. Calder et al. analyzed Microsoft's CDN, known as Azure, as a representative example of an anycast CDN [26].

IXPs have also received a great deal of attention in the research and operational literature during the last decade. During the 2000s, IXPs were in part responsible for a *peering revolution*, offering neutral points for ASes to establish settlement-free peering agreements. IXPs encourage peering in order to keep traffic local and to avoid reaching local neighbors via either paid transit links or longer circuitous routes [3]. A well documented phenomenon is that the proliferation of IXPs has contributed to a *flattening* of the Internet [14], with hundreds of IXPs spread all over the world facilitating connectivity between thousands of co-located networks. In the research literature, a number of papers have studied the anatomy of large IXPs [6] as well as the role of IXPs in developing regions [27], [28].

Recently, Geoff Huston observed the wide-ranging effects of the flattening structure of the Internet and the rise of CPs [4]. Huston suggests that these trends are marginalizing the role of Transit Providers, terming this as *"The Death of Transit"*.

There is a vast body of previous literature on applying graph theoretic concepts to study the AS graph structure. Some examples of such work are papers that have introduced k-core decomposition to study properties of the network [29]–[31]. These works mainly take a mathematical perspective about the structure of the AS graph. In this work, we also utilize the k-core decomposition technique from graph theory to study the role specifically of CPs in the Internet over the years. However, we pair the graph-theoretic concept with domain knowledge, insights from other measurement datasets, and documented strategies and actions of the CPs themselves, which gives further context and explanation for the observed phenomenon.

III. Methodology and dataset

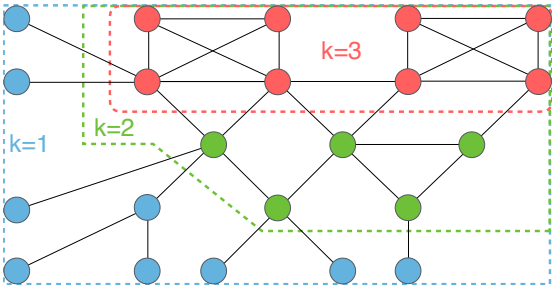


Fig. 1. Example of a k-core decomposition of a given graph.

k-core decomposition: Our goal is to study changes in the structure of the AS-level Internet ecosystem from the perspective of content providers and CDNs, specifically, whether large CPs are now part of the core of the network, and the historical evolution of when such a transition occurred. For this purpose, it is necessary to define a methodology to determine which ASes are part of the core of the network.

We refer to the *core* of the network as the subset of ASes that are densely connected. To compute the set of such ASes, we use k-core decomposition, a naturally applicable tool from the graph-theoretic literature. Although simpler graph metrics, such as node degree, may indicate whether an AS is densely connected or not, these metrics are not as robust as the k-core. For instance, to define the core using node degree, it would be necessary to set a threshold, while the k-core inherently defines a *community* of densely connected nodes.

A k-core of a graph $\mathcal{G}$ is the maximum induced subgraph in which all the vertices have at least degree k (see [32]). A vertex or node that belongs to a k-core has at least k neighbors which all have degree at least k. Moreover, a node that belongs to core k also belongs to any core $j < k$, thus the shell-index is given by the maximum core that a node belongs to. Figure 1 displays k-cores using a small graph example where nodes are colored to indicate their shell-index. As the figure shows, the shell-index (or simply "core") is given by the degree of the node as well as the degree of the neighbors in the induced graph. This can be seen in the example where some four-degree nodes are in core 2 while nodes of degree 3 are in core 3. Furthermore, AS graphs are *core-connected* [33], which means that there are k different paths between two ASes of the same k-core.

The central part of the network is made of ASes that belong to the maximum core k_{max}. In our analysis we study the evolution of cores of the CPs. However, the k_{max} as well as the k-indices of the AS graph change over time. For this reason, we normalize k in each snapshot by its k_{max} index, which leads to a normalized k with values between 0 and 1, referred to as k^*. For now on, TOPcore will refer to $k^* = 1$. To calculate k-core decomposition on each snapshot of an AS graph we used two tools, LaNet-vi [33], which also provides network visualization, and NetworkX, a python library.

AS graph datasets: To apply the above k-core decomposition methodology on the Internet graph longitudinally,

we need periodic historical snapshots of the Internet's AS-level topology. We rely on publicly available AS topology snapshots from CAIDA. CAIDA curates AS topology data from both BGP and traceroute-derived sources. The BGP AS relationship dataset ([1]) is derived from BGP dumps taken from RouteViews and RIPE RIS collectors [34] from 1998 to present, and contains AS links observed at the BGP collectors along with an inferred business relationships. We use a second dataset which consists of AS links extracted from traceroutes from CAIDA's Archipelago [35] vantage points towards every routed /24 prefix[2]. The two datasets can provide somewhat different views of the Internet's AS-level topology. While the number of edges in each BGP data snapshot is larger than in traceroute data snapshots, traceroute often reveals peer-to-peer links which are not seen at BGP collectors [36]. To get the most complete picture of AS-level connectivity, we chose to combine data from both the BGP and Ark datasets, which we refer to as the "Ark+BGP" dataset. This dataset consists of monthly snapshots dating from 1998 to present, which is sufficiently long to detect the evolution of the number of peers of CPs. To view the *k*-core decomposition using only the BGP dataset or traceroute dataset, we refer the reader to a website with these visualizations.[3]

A limitation of our methodology is that CPs also serve content from caches located within ISPs [12], [25], which are not visible as AS links in BGP or traceroute. Even CPs that follow an in-network caching strategy, however, generally need to peer in order to reach ISPs that are not willing to host caches in their networks, to fill the caches, and to serve dynamic content that cannot be cached. In this work we only study the evolution of AS-level connectivity of CPs; we leave an analysis of cache infrastructure to future work.

IV. A first look into the core evolution of CPs

A well-documented trend in the evolution of the Internet is that the set of ASes responsible for generating most of the traffic has been shrinking; recent studies have shown that only few tens of ASes together generate most of the traffic, while in the past that number was in the thousands [1], [37]. Given this trend toward traffic consolidation, we track the core evolution of seven big players, which we refer to as the *Big Seven*: Akamai (AS20940), Amazon (AS16509), Apple (AS714), Facebook (AS32934), Google (AS15169), Microsoft (AS8075) and Netflix (AS2906). Although CPs may have more than one ASN, we study the evolution of their primary ASNs. Publicly available AS sibling datasets can be incomplete and need semi-manual verification; we leave a consideration of sibling ASes for future work.

We chose these CPs based on publicly available information such as PeeringDB [38] and Sandvine reports [39]. According to their PeeringDB records, Akamai, Facebook and Netflix have heavily outbound traffic with levels over 10 Tbps, 1 Tbps and 1 Tbps, respectively. In addition, Sandvine reported in 2016 that Netflix dominated the peak period traffic with 35% of the traffic share, followed by YouTube with 17% and Amazon Video with 4% [39] in North America. The report also mentioned that FaceTime and iCloud (Apple) and Skype and Xbox (Microsoft) are among the top sources of peak period traffic. Cloud computing is also responsible for large data transfers, and this market is led by Amazon with 42% of the share, Microsoft 15% and Google 7% [40].

Our *a priori* hypothesis is that all of these CPs currently belong to the TOPcore. We check whether our hypothesis is true, and if so, *when* and *how quickly* they reached the TOPcore. We then attempt to dig deeper into the reasons why we observe these CPs in the TOPcore, and correlate with external factors such as legal disputes, market expansions, QoE improvements, services releases etc. to explain why the CPs appeared in the TOPcore at a certain time.

We also investigate whether CPs belong to the TOPcore in each geographical region, defined as the Regional Internet Registries (RIR) regions. We repeat the analysis of speed and date of arrival for each CP in every RIR with a focus on detecting differences by region, especially systematic delays in when certain CPs appeared in specific regions.

A. Tracking the evolution of the Big Seven

Figure 2 shows the monthly evolution of the normalized CP-core on the Ark+BGP dataset. A first observation is that as of the end of 2017, all the studied CPs have already joined the TOPcore, which is indicated by the fact that the normalized core value for each CP is 1.

There appear to be two groups among the studied CPs, one composed of Akamai, Google and Microsoft which reached the TOPcore by 2005, and another comprising Amazon, Apple, Facebook and Netflix, which became members of the TOPcore between 2010 and 2015. The CPs in the first group are arguably more established, and have been providing a variety of online services for many years. The second group consists of CPs that at some point decided to deploy their own infrastructure and stop serving content using third-party CDNs [41] as multimedia content began to dominate the Internet traffic share [42]. Moreover, the transition from lower cores to upper cores among the members of the latter group is faster than in the former group. The fast evolution of Amazon, Apple, Facebook and Netflix cores is likely to have been encouraged by the vast number of peering facilities which appeared during the last decade [3], [43].

Next we dig deeper into the evolution of CPs individually. Specifically, we attempt to correlate the topological characteristics of the CPs (their core) with business strategies, acquisitions, or other factors which could explain why the CP entered the TOPcore.

a) Akamai: Akamai has been in the TOPcore since 2005. Akamai is a *pioneer* in content-delivery, and since its business model relies on providing high-availability low-latency hosting

[1]CAIDA's BGP serial-1 dataset:http://data.caida.org/datasets/as-relationships/serial-1/

[2]The Ark dataset was merged with skitter dataset http://data.caida.org/datasets/topology/skitter-aslinks/.

[3]Graph visualization website:http://cnet.fi.uba.ar/TMA2018/.

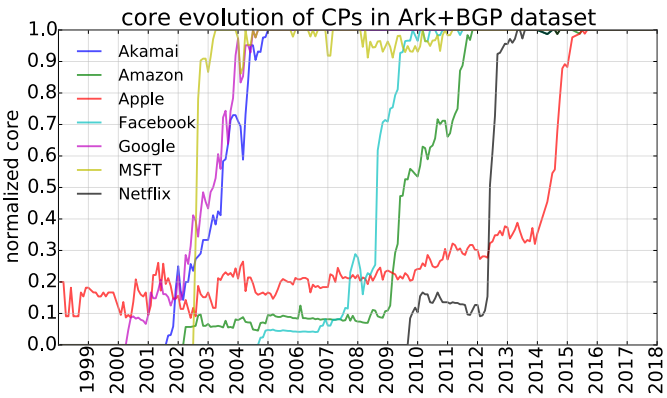


Fig. 2. k-core evolution of the *Big Seven*. All of these CPs have reached the TOPcore.

rather than generating content, they have always aimed to have a large number of peers. Moreover, Akamai acquired Speedera networks, a rival third-party CDN, in 2005 to consolidate its market position as well as to enlarge its platform. According to Figure 2, Akamai had already reached the TOPcore when it purchased Speedera networks.

b) Amazon: Amazon's infrastructure deployment appears to have occurred in two steps, according to Figure 2. This is further corroborated by information provided on Amazon's website [44]. In 2009 Amazon established its datacenter in Northern California, which matches with the first growth. Between 2010 and 2012, Amazon established datacenters in several parts of the world, which would explain the second growth spurt from 2010 to 2012. In addition to the datacenter deployment, Amazon established dozens of PoPs all over the world to boost expansion, which correlates with its rise to the TOPcore. Finally, we find that the WHOIS record for Amazon's DNS nameservers zone (e.g. `awsdns-39.net`) was created in late 2010, which coincides with the last spurt in its core growth. DNS nameservers are essential elements of Amazon's cloud infrastructure, required to load balance traffic among locations. For instance, Slack, which is hosted on Amazon, has `slack.com` NS records pointing to `ns-606.awsdns-11.net` among other AWS nameservers.

c) Apple: We find that Apple's AS reached the TOPcore in 2015 after a fairly quick growth. According to publicly documented information, Apple has been steadily off-loading its content from Akamai onto its own CDN since 2013 [45]. Apple's traffic share has been growing rapidly in recent years fueled by large data transfers due to software updates, such a new OS releases [46] or security patches. This is one of the motivating reasons for Apple to build its own CDN. Further, the company has recently announced that is planning to break into the TV market, producing original television shows, which will be served from Apple's CDN [47].

d) Facebook: Facebook's AS32934 got close to the TOPcore in 2010 after a rapid growth in its normalized core between 2008 and 2010. The number of users on Facebook grew exponentially from 12M in December 2006 to 350M by the end of 2009 [48] which coincides with Facebook's expansion period and rise to the TOPcore. Although Facebook has kept on growing exponentially since then, the massive growth during that period encouraged Facebook to establish multiple peering agreements that enabled it to reach the TOPcore. In addition, the WHOIS record for `fbcdn.net`, which stands for Facebook CDN, was created in 2007 when Facebook's expansion was happening.

e) Google: Google was launched in September 1997 and in just a couple of years became the most popular search engine [49]. Over time, as Google started serving large volumes of video traffic via the acquisition of YouTube in 2006 [50], it expanded its CDN to get as close as possible to "eyeball" networks and achieve high QoE for users. However, looking carefully into Google's peers in the early days, between 1999 and 2003, even before the CDN was deployed, it had several agreements with tier-1 transit providers. Before December 2002, Google already peered with Level3 (AS3549), TATA (AS6453), Telstra (AS4637), NTT (AS2914), Zayo (AS6461), Qwest (AS209), GTT (AS3257) and Cogent (AS174). Links with a number of large Transit Providers resulted in Google becoming part of the same core level as those transit providers.

f) Microsoft: Similar to Google, Microsoft has been serving large volumes of online content since the mid-1990s, such as hotmail and MSN. Figure 2 shows that Microsoft entered the TOPcore in late 2002. An analysis of Microsoft's peers shows that by December 2002, Microsoft had a large number of connections with tier-1 Transit Providers, e.g., Level3 (AS3549), TATA (AS6453), Telia (AS1299), Telefonica (AS12956), Sprint (AS1239) and NTT (AS2914). The presence of peering links with multiple tier-1 ASes which were in the TOPcore resulted in Microsoft also entering the TOPcore.

g) Netflix: In 2012, it took Netflix less than a year to move from core $k^* = 0.1$ to the TOPcore. Netflix started to offer video streaming in 2007 using third-party CDNs and transit providers. With the growing popularity of the service and increasing traffic volumes, the company moved content to its own Open Connect [51] platform in 2012. Netflix's strategy to switch from third-party CDNs to its own infrastructure manifests itself as a sharp increase in its normalized core value between 01/2012 and 09/2012 as shown in Figure 2. The transition of Netflix from using third-party CDNs to using its OpenConnect platform also led to a number of peering disputes with large access providers over interconnection fees, e.g., with Comcast in 2013 [52].

In summary, all of the studied CPs moved from third-party CDNs to private CDNs and entered the TOPcore. In particular, Apple, Facebook, Microsoft and Netflix all off-loaded content from Akamai. These changes led to significant loss of revenue for Akamai and a drop in its share price [41]. Despite losing major clients, Figure 2 shows that Akamai is still in the TOPcore, which means that Akamai's peering agreements do not depend exclusively on these large clients.

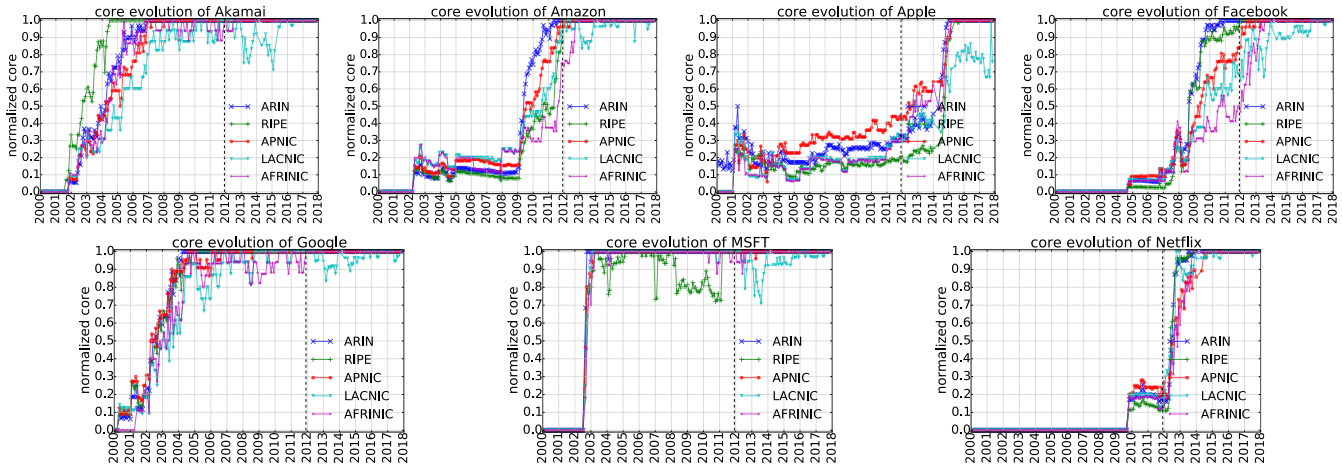


Fig. 3. k-core evolution of the *Big Seven* in each RIR. The dashed line displays the beginning of NetAcuity geolocation database.

B. Evolution by geographical region

Next, we compare the evolution of the *Big Seven* by geographical region. To determine which regions an AS is present in, we use the NetAcuity [53] geolocation database to geolocate each prefix advertised by an AS in a given snapshot. The (in)accuracy of geolocation databases has been studied extensively [54]. However, previous work has found that the NetAcuity database is mostly reliable for country-level geolocation [55]. We use RIR-level granularity in this work, so we believe that this analysis is not affected by inaccuracies in geolocation. After geolocating ASes, we combine the monthly "Ark+BGP" snapshots with the mapping between AS and RIR to create monthly RIR subgraphs.

There are two issues with this basic methodology that we need to account for. First, we need AS geolocation information throughout the duration of "Ark+BGP" dataset. However, CAIDA only had NetAcuity records since November 2011, while our topology dataset starts in January 1998. Second, NetAcuity appears to incur a time lag between when a prefix is active in a new location and when it appears at that location in the database. For example, NetAcuity started reporting the presence of Netflix in the LACNIC region in December 2016, while a June 2015 Wayback Machine snapshot [4] already showed Netflix as a member of a Brazilian IXP. As our goal is to track historical evolution, it is necessary to include an AS in the RIR subgraph when changes are actually happening and not once they have already happened. To account for these issues we made two modifications to the basic methodology.

1) We assume that the 7 CPs we study have always had a presence in every RIR. While building the RIR subgraph, however, we only include observed connectivity between the CPs and other ASes geolocated to the RIR.
2) We assume that prior to November 2011 (the start of our Netacuity dataset), ASes had the same locations that they had in November 2011.

[4]Wayback Machine snapshot of members of Brazilian IXP. 06/2015:http://web.archive.org/web/20150617231252/http://ix.br/particip/sp

While this methodology allows us to create RIR subgraphs, we cannot infer where the connection between two ASes actually happens when those ASes have presence in multiple RIR subgraphs. For instance, Google and Level3, which are currently present in every RIR subgraph, may not have a physical link in each RIR.

1) Geographical evolution of the Big Seven: Figure 3 shows the evolution of each CP by RIR. We find that all CPs have reached the TOPcore in every RIR although the arrival date varies by CP and RIR.

Amazon and Facebook show differences between RIRs in their growth in the late 2000s and early 2010s. Amazon first established datacenters and PoPs in the US before 2009, then expanded to Singapore (APNIC) in 2010, Brazil (LACNIC) in 2011, and several locations in Europe (RIPE) in 2011 [44]. Figure 3 shows that Amazon's core trends follow its documented infrastructure deployment. Facebook, which has been part of the worldwide TOPcore since 2009, lagged in APNIC, LACNIC and AFRINIC, where it got to the TOPcore several years after ARIN and RIPE. Facebook got to the TOPcore in ARIN in August 2010, APNIC in August 2012, LACNIC in August 2013 and in AFRINIC in March 2013. In RIPE, Facebook has been in the upper cores ($k^* \geq 0.9$) since early 2010, however, it finally reached the TOPcore in January 2012. Facebook publicly acknowledged its lack of presence in developing regions and took steps to correct in order to improve user QoE in those regions [56].

Since the *Big Seven* are all U.S. based companies, one might expect that they first reached the TOPcore in ARIN, and later expanded to developing regions such as LACNIC and AFRINIC. Figure 3 shows, however, that Akamai, Google and Microsoft showed negligible differences across RIRs in the early 2000s, which does not match documented information about their CDN deployment. For instance, Google established a PoP in Argentina only in 2011 [57]. The reason for this discrepancy is that Akamai, Google and Microsoft had peering links with tier-1 transit providers present in those regions,

TABLE I
PERCENTAGE OF LOCAL PEERS IN EACH REGION

	%	Akamai	Amazon	Apple	Facebook	Google	MSFT	Netflix
ARIN	2007	0.33	1.0	0.73	0.51	1.0	0.68	0
	2012	0.45	0.49	0.6	0.49	0.43	0.52	**0.86**
	2017	0.41	0.4	0.42	0.44	0.39	0.43	0.39
RIPE	2007	0.75	0.0	0.0	0.68	0.0	0.42	0
	2012	0.74	**0.75**	0.15	0.75	**0.81**	**0.76**	0.14
	2017	0.71	0.68	**0.67**	0.73	0.7	0.7	**0.77**
APNIC	2007	0.21	0.0	0.4	0.21	0.0	0.13	0
	2012	**0.45**	**0.24**	0.29	0.37	0.27	0.24	0.0
	2017	0.47	0.37	0.4	0.37	**0.38**	**0.37**	**0.39**
LACNIC	2007	0.0	0.0	0.0	0.11	0.0	0.0	0
	2012	0.11	**0.35**	0.0	0.36	0.07	0.08	0.0
	2017	**0.56**	0.53	**0.17**	**0.51**	**0.56**	**0.5**	**0.57**
AFRINIC	2007	0.05	0.0	0.0	0.11	0.0	0.04	0
	2012	0.0	0.0	0.0	0.05	0.0	0.0	0.0
	2017	**0.23**	0.03	0.07	**0.14**	**0.07**	**0.1**	**0.1**

which caused the CPs to be in the TOPcore of those regions as well. A look at peering relationships in the early 2000s confirms this hypothesis — Google was not present in the LACNIC region, however, it peered with Level3 (AS3549), TATA (AS6453) and Qwest (AS209), which were present in LACNIC. We confirmed that the tier-1 ASes were present in LACNIC because they peered with the two largest Argentinian ISPs, Cablevision (AS10318) and TASA (AS4926), which were only present in Argentina at the time.

Netflix and Apple were the latest to enter the worldwide TOPcore as well as the TOPcore of each RIR. Netflix was in the lower cores ($k^* < 0.3$) in every RIR in January 2012. By January 2014 it moved to the TOPcore in every RIR. Apple's growth was similar — in June 2014 it was in cores lower than 0.5. One year later it was in the TOPcore of every RIR except LACNIC where it reached the TOPcore in Jan 2017.

2) Local Peers: The analysis of the previous section showed that core evolution does not necessarily reflect the geographical expansion of CPs. Here we present a complementary analysis. Table I shows the percentage of peers of a CP in a region that are registered in that region (according to WHOIS records). For example, Google had 38% of local peers in APNIC in 2017, meaning that 38% of Google's links with ASes present in APNIC were with ASes registered in APNIC, while the remaining 62% were with ASes present in APNIC but registered elsewhere. This metric provides information about when a CP first arrived in a region, as that would intuitively lead to an increase in the local peering metric.

Table I shows that Akamai, Google and Microsoft significantly increased the number of local peers in Latin America (LACNIC) in the last five years. APNIC has also shown a growth in the number of local peers, but slower than in LACNIC. In contrast to Figure 3 where all of the CPs belong to every TOPcore, Table I shows a fairly low number of local peers of these CPs in AFRINIC. As of 2017, Akamai had the largest fraction with 0.23, Facebook second with 0.14 and all the rest were under 0.10.

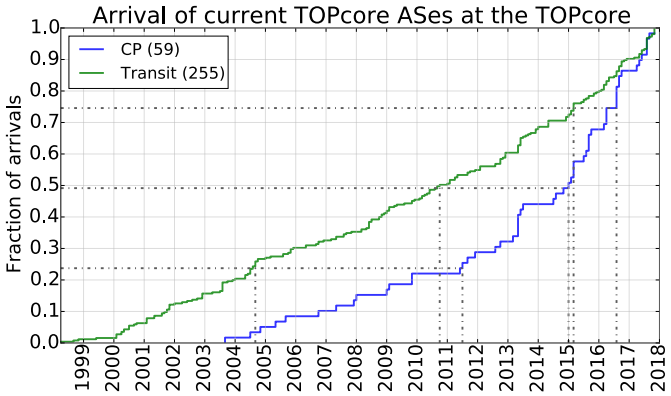


Fig. 4. Date of first arrival at the TOPcore for ASes which currently compose the TOPcore.

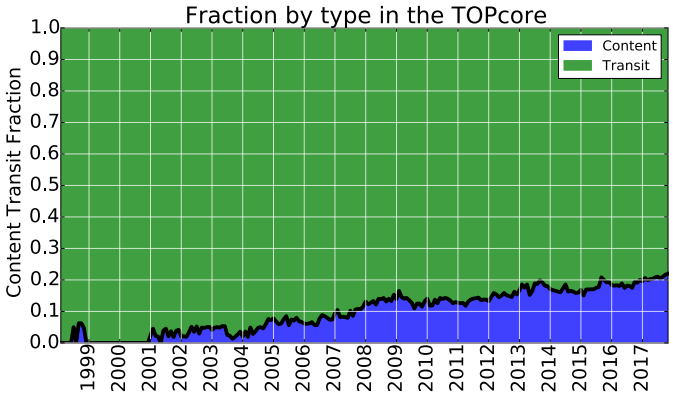


Fig. 5. Monthly evolution of the fraction of CPs and Transit in the TOPcore.

While the percentage of local peers of CPs increases over the years in regions where they initially had a small fraction of local peers, ARIN shows the opposite trend. This is likely because the studied CPs are U.S. companies. Consequently, their number of local peers in ARIN saturates, while the number of non-local peers increases as companies outside the U.S. deploy infrastructure in ARIN and peer with the CPs.

V. THE TOPCORE BEYOND THE BIG SEVEN

We conclude our analysis by looking at other networks in the TOPcore. Specifically, we investigate how many networks are in the TOPcore, what type of networks they are (transit or content), what fraction of the TOPcore networks are accounted for by content networks, and *how quickly* those networks reached the TOPcore. To identify ASes in the TOPcore, we use the criterion that an AS must be in $k^* > 0.975$ at any point in time, and in $k^* \geq 0.95$ during the last six months of our dataset (Mar-2017 to Oct-2017). Note that this definition of the TOPcore is broader than that used in the previous section where the criterion for belonging to the TOPcore was $k^* = 1$. By this broader definition, we had 314 ASes in the TOPcore — 59 Content Providers and 255 Transit/Access Providers according to CAIDA's AS classification [58].

TABLE II
ORIGIN ACCORDING TO WHOIS FOR TOPCORE ASES

	ARIN	RIPE	APNIC	LACNIC	AFRINIC	Unknown
Content	36	20	3	0	0	-
Transit	35	165	38	3	8	6

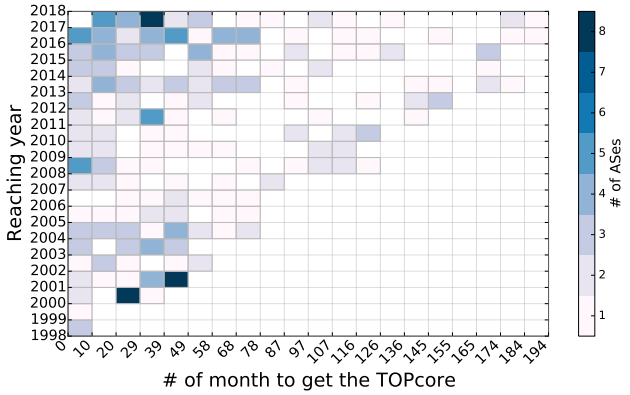


Fig. 6. Correlation between speed of growth and date of arrival at the TOPcore.

Figure 4 shows the fraction of these 314 ASes (separated into Content and Transit) that first reached the TOPcore over time. This plot clearly shows that over time, more CPs have been peering aggressively and joining the TOPcore. Interestingly, 75% of the CPs in the studied set first entered the TOPcore after 2011. Moreover, we see two distinct phases in the CP curve — the rate at which CPs arrive in the TOPcore has increased since 2011. The arrival of Transit Providers, on the other hand, appears steady over the years.

Table II shows the geographical distribution of ASes in the TOPcore. We see that CPs in the TOPcore are mostly from ARIN and RIPE (with the exception of 3 from APNIC). However, among Transit Providers, RIPE has significantly more ASes than other regions. AFRINIC and LACNIC have negligible or no presence in either category. APNIC has a considerable number of Transit Providers but few CPs.

Figure 6 shows a heatmap of the number of ASes that arrived at the TOPcore at a certain time and at a certain *speed*. We define *speed* as the number of months to move from $k^* = 0.3$ to $k^* = 0.975$, and this definition is based on the transitions from lower to upper cores seen in Figure 2. Figure 6 shows that 172 of the 314 ASes joined the TOPcore between 2011 and 2018 and most of them moved from lower cores in just a few months, where the average speed was 61 months. This fast evolution of the TOPcore in recent years can be possibly explained by the growth of the number of peering facilities and participants at those facilities in this time frame.

Next, we investigate the composition of ASes in the TOPcore over time. In Figure 5, we applied the TOPcore criterion to determine which ASes belong to the TOPcore every month, and then classified the ASes in the TOPcore as Content or Transit. We find that the fraction of CPs in the TOPcore has been steadily increasing; as of the October 2017 snaspshot,

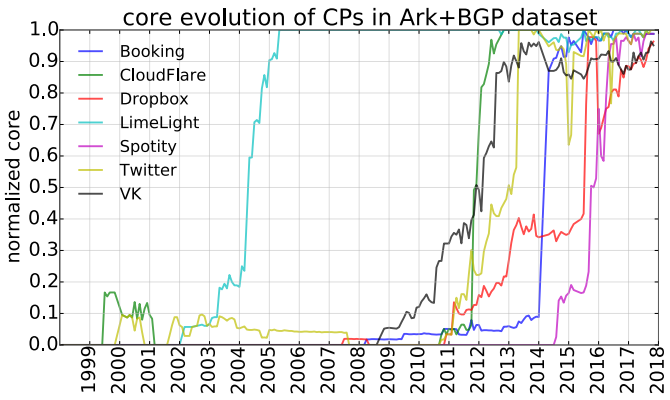


Fig. 7. k-core evolution of CPs other than the *Big Seven*.

22% of ASes in the TOPcore were CPs. Note that the absolute number of ASes in the TOPcore has been increasing as well, which implies that the TOPcore has been incorporating more CPs than Transit ASes over time.

Finally, Figure 7 shows the evolution of seven CPs that have joined the TOPcore in recent years (different from the Big Seven). Interestingly, there are ASes in this set that are not normally considered among the top CPs, such as Booking.com or Spotify. We believe that analysis of core evolution can be a possible tool to identify ASes that are increasing in significance, the so-called "up and coming" CPs. We refer the reader to the following website to replicate our results:http://cnet.fi.uba.ar/TMA2018/

VI. CONCLUSIONS

In this work we demonstrated that CPs have taken a decisive role in the AS ecosystem, where seven large companies in the Internet content market have moved towards the core of the network. By analyzing the evolution of the cores of the CPs, we were able to identify possible reasons related to business practices, strategies, and geographical expansion that explain the rise of these networks to the top core. Furthermore, we showed the core of the network has been rapidly incorporating content ASes over time.

VII. ACKNOWLEDGMENTS

This work was partially founded by UBACyT 2014 (20020130200122BA) and NSF grant CNS-1513847. EC acknowledges CONICET Argentina for a PhD fellowship.

REFERENCES

[1] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet inter-domain traffic," in *ACM SIGCOMM*. ACM, 2010.
[2] K. C. Claffy, G. C. Polyzos, and H.-W. Braun, "Traffic characteristics of the t1 nsfnet backbone," in *INFOCOM'93*. IEEE, 1993.
[3] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "There is more to IXPs than meets the eye," *ACM SIGCOMM CCR*, 2013.
[4] G. Huston, "The death of Transit,," 2016.
[5] P. Gill, M. Arlitt, Z. Li, and A. Mahanti, "The flattening internet topology: Natural evolution, unsightly barnacles or contrived collapse?" in *Proceedings of PAM*. Springer, 2008.

[6] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a large european ixp," in *Proceedings of ACM SIGCOMM*, 2012.

[7] T. Leighton, "Improving performance on the internet," *Comm. of the ACM*, vol. 52, no. 2, pp. 44–51, 2009.

[8] Wired, "Google and Netflix Make Land Grab On Edge Of Internet," https://www.wired.com/2012/06/cdn/, 2016.

[9] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu *et al.*, "B4: Experience with a globally-deployed software defined wan," *ACM SIGCOMM CCR*, vol. 43, no. 4, pp. 3–14, 2013.

[10] D. E. Eisenbud, C. Yi, C. Contavalli, C. Smith, R. Kononov, E. Mann-Hielscher, A. Cilingiroglu, B. Cheyney, W. Shang, and J. D. Hosein, "Maglev: A fast and reliable software network load balancer." in *NSDI*, 2016.

[11] B. Schlinker, H. Kim, T. Cui, E. Katz-Bassett, H. V. Madhyastha, I. Cunha, J. Quinn, S. Hasan, P. Lapukhov, and H. Zeng, "Engineering egress with edge fabric: Steering oceans of content to the world," in *Proceedings of ACM SIGCOMM*, 2017.

[12] A.-J. Su, D. R. Choffnes, A. Kuzmanovic, and F. E. Bustamante, "Drafting behind akamai: Inferring network conditions based on cdn redirections," *IEEE/ACM ToN*, vol. 17, no. 6, pp. 1752–1765, 2009.

[13] N. Economides and J. Tåg, "Network neutrality on the internet: A two-sided market analysis," *Information Economics and Policy*, vol. 24, no. 2, pp. 91–104, 2012.

[14] A. Dhamdhere and C. Dovrolis, "The internet is flat: Modeling the transition from a transit hierarchy to a peering mesh," in *Proceedings of ACM CoNEXT*. ACM, 2010.

[15] ——, "Ten years in the evolution of the internet ecosystem," in *Proceedings of ACM IMC*, 2008.

[16] P. Faratin, "Economics of overlay networks: An industrial organization perspective on network economics," in *Proceedings of the NetEcon+ IBC workshop*, 2007.

[17] J. Dilley, B. Maggs, J. Parikh, H. Prokop, R. Sitaraman, and B. Weihl, "Globally distributed content delivery," *IEEE Internet Computing*, vol. 6, no. 5, pp. 50–58, 2002.

[18] G. Pallis and A. Vakali, "Insight and perspectives for content delivery networks," *Comm. of the ACM*, vol. 49, no. 1, pp. 101–106, 2006.

[19] C. Huang, A. Wang, J. Li, and K. W. Ross, "Understanding hybrid cdn-p2p: why limelight needs its own red swoosh," in *Proceedings of NOSSDAV*, 2008.

[20] M. Pathan, R. Buyya, and A. Vakali, "Content delivery networks: State of the art, insights, and imperatives," *Content Delivery Networks*, pp. 3–32, 2008.

[21] M. Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, and R. Govindan, "Mapping the expansion of google's serving infrastructure," in *Proceedings of ACM IMC*, 2013.

[22] P. Casas, A. D'Alconzo, P. Fiadino, A. Bär, A. Finamore, and T. Zseby, "When youtube does not work?analysis of qoe-relevant degradation in google cdn traffic," *IEEE TNSM*, vol. 11, no. 4, 2014.

[23] Q. Huang, K. Birman, R. van Renesse, W. Lloyd, S. Kumar, and H. C. Li, "An analysis of facebook photo caching," in *Proceedings of ACM SOSP*, 2013.

[24] Y.-W. E. Sung, X. Tie, S. H. Wong, and H. Zeng, "Robotron: Top-down network management at facebook scale," in *Proceedings of ACM SIGCOMM*, 2016.

[25] T. Böttger, F. Cuadrado, G. Tyson, I. Castro, and S. Uhlig, "A hyper-giant's view of the internet," *ACM SIGCOMM CCR*, 2017.

[26] M. Calder, A. Flavel, E. Katz-Bassett, R. Mahajan, and J. Padhye, "Analyzing the performance of an anycast cdn," in *Proceedings of ACM IMC*, 2015.

[27] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett, "Peering at the internet's frontier: A first look at isp interconnectivity in africa." in *PAM*, 2014.

[28] R. Fanou, P. Francois, and E. Aben, "On the diversity of interdomain routing in africa," in *PAM*, 2015.

[29] J. I. Alvarez-Hamelin, L. Dall'Asta, A. Barrat, and A. Vespignani, "K-core decomposition of Internet graphs: hierarchies, self-similarity and measurement biases," *Networks and Heterogeneous Media*, vol. 3, no. 2, pp. 371–293, 2008.

[30] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "K-core organization of complex networks," *Phys. Rev. Lett.*, vol. 96, no. 4, p. 040601, 2006.

[31] C. Orsini, E. Gregori, L. Lenzini, and D. Krioukov, "Evolution of the internet k-dense structure," *IEEE/ACM ToN*, vol. 22, no. 6, pp. 1769–1780, Dec. 2014.

[32] V. Batagelj and M. Zaveršnik, "Fast algorithms for determining (generalized) core groups in social networks," *Advances in Data Analysis and Classification*, vol. 5, no. 2, pp. 129–145, 2011.

[33] M. G. Beiró, J. I. Alvarez-Hamelin, and J. R. Busch, "A low complexity visualization tool that helps to perform complex systems analysis," *New J. Phys*, vol. 10, no. 12, p. 125003, 2008.

[34] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and k. claffy, "As relationships, customer cones, and validation," in *Proceedings of ACM SIGCOMM IMC*, 2013.

[35] CAIDA, "Archipelago (Ark) Measurement Infrastructure," https://www.caida.org/projects/ark/.

[36] Y. Hyun, A. Broido *et al.*, "Traceroute and bgp as path incongruities," 2003.

[37] Stefan Meinders, "The New Internet," ENOG11, 2016.

[38] PeeringDB, "https://www.peeringdb.com."

[39] Sandvine, "Global internet phenomena report 2016," 2016.

[40] USA Today, "Does Amazon control the Internet, or does it just feel that way?" https://www.usatoday.com/story/tech/talkingtech/2017/03/01/amazon-control-internet-aws-cloud-services-outage/98548762/, 2017.

[41] Seeking Alpha, "Apple, Microsoft And Facebook Bring More Traffic To In-House CDNs, Impacting Akamai's Media Business," https://seekingalpha.com/article/3613736-apple-microsoft-facebook-bring-traffic-house-cdns-impacting-akamais-media-business, 2015.

[42] Sandvine, "Global internet phenomena report Spring 2011," 2011.

[43] V. Stocker, G. Smaragdakis, W. Lehr, and S. Bauer, "The growing complexity of content delivery networks: Challenges and implications for the internet ecosystem," *Telecommunications Policy*, vol. 41, no. 10, pp. 1003–1016, 2017.

[44] Amazon, "AWS global infrastructure," https://aws.amazon.com/es/about-aws/global-infrastructure/, 2017.

[45] Apple Insider, "Apple's in-house CDN efforts spell trouble for Akamai as infrastructure biz warns of losses," http://appleinsider.com/articles/16/02/10/apples-in-house-cdn-efforts-spell-trouble-for-akamai-as-infrastructure-biz-warns-of-losses, 2016.

[46] ARS Technica, "Apple?s multi-terabit, $100M CDN is live - with paid connection to Comcast," https://arstechnica.com/information-technology/2014/07/apples-multi-terabit-100m-cdn-is-live-with-paid-connection-to-comcast/, 2014.

[47] LA Times, "Apple's original TV production to begin small: 'We are just starting out'," http://beta.latimes.com/business/hollywood/la-fi-ct-apple-television-strategy-planet-apps-20170214-story.html, 2017.

[48] Yahoo Finance, "Number of active users at Facebook over the years," https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html, 2012.

[49] Tom Hormby, "The Rise of Google: Beating Yahoo at Its Own Game," http://lowendmac.com/2013/the-rise-of-google-beating-yahoo-at-its-own-game/.

[50] New York Times, "Google to Acquire YouTube for $1.65 Billion," http://www.nytimes.com/2006/10/09/business/09cnd-deal.html.

[51] Netflix Media Center, ""Announcing the Netflix Open Connect Network"," https://media.netflix.com/en/company-blog/announcing-the-netflix-open-connect-network, 2012.

[52] Quartz Media, ""The inside story of how Netflix came to pay Comcast for internet traffic"," https://qz.com/256586/the-inside-story-of-how-netflix-came-to-pay-comcast-for-internet-traffic/, 2014.

[53] Digital Element, "NetAcuity," https://www.digitalelement.com/solutions/.

[54] Poese, Ingmar and Uhlig, Steve and Kaafar, Mohamed Ali and Donnet, Benoit and Gueye, Bamba, "IP geolocation databases: Unreliable?" *ACM SIGCOMM CCR*, vol. 41, no. 2, 2011.

[55] Gharaibeh, Manaf and Shah, Anant and Huffaker, Bradley and Zhang, Han and Ensafi, Roya and Papadopoulos, Christos, "A look at router geolocation in public and commercial databases," in *Proceedings of ACM SIGCOMM IMC*, 2017.

[56] Quinn, James, "Being Open: How Facebook Got It's Edge," *NANOG68*, 2016.

[57] Galperin, Hernan, "Connectivity in Latin America and the Caribbean: The role of internet exchange points," *Internet Society, November*, 2013.

[58] CAIDA, "CAIDA's AS classification list," http://data.caida.org/datasets/as-classification/.

Studying the Evolution of Content Providers in IPv4 and IPv6 Internet Cores

Esteban Carisimo[a,b], Carlos Selmo[c], J. Ignacio Alvarez-Hamelin[a,b], Amogh Dhamdhere[d]

[a] *Universidad de Buenos Aires*
[b] *CONICET*
[c] *Instituto Tecnológico de Buenos Aires*
[d] *CAIDA, San Diego Supercomputer Center, UC San Diego*

Abstract

There is recent evidence that the core of the Internet, which was formerly dominated by large transit providers, has been reshaped after the transition to a multimedia-oriented network, first by general-purpose CDNs and now by private CDNs. In this work we use k-cores, an element of graph theory, to define which ASes compose the core of the Internet and to track the evolution of the core since 1999. Specifically, we investigate whether large players in the Internet content and CDN ecosystem belong to the core and, if so, since when. In addition, we examine differences between the IPv4 and IPv6 cores. We further investigate regional differences in the evolution of large content providers. Finally, we show that the core of the Internet has incorporated an increasing number of content ASes in recent years. To enable reproducibility of this work, we provide a website to allow interactive analysis of our datasets to detect, for example, "up and coming" ASes using customized queries.

Keywords:
Content Providers, CDNs, topology, k-cores

1. Introduction

The structure of the Autonomous System (AS) network has been changing over the years driven by disruptive changes on the Internet [1]. In the NSFNET era, the Internet had a monolithic backbone deployed in the U.S. to interconnect research and educational institutions [2]. After the US government decommissioned the NSFNET, the interdomain network moved onto a Transit era where the network had a hierarchical structure [1, 3]. More recently, the Internet has transformed into multimedia network, driven by high bandwidth demands and low latency requirements, resulting in a Content era [4].

Content Delivery Networks (CDNs) have played a decisive role in the evolution towards a multimedia network [5] and the resulting *flattening* of the Internet [1, 6]. CDNs are decentralized serving infrastructures that provide front-ends close to users to reduce latency, maximize the throughput and avoid delivering packets through long routes, which increase latency and can be congested [7]. CDNs typically establish a large number of peering agreements with ASes hosting customers of their content ("eyeballs"). It is not necessary that every Content Provider (CP) needs to deploys its own CDN. A number of *third-party CDNs* provide hosting services without being content generators, such as Akamai and LimeLight. However, it is apparent that several CPs have transformed into private CDNs with worldwide coverage instead of delivering content through Transit Providers or third-party CDNs due to a range of technical, economic, and legal reasons [8, 9, 10, 11, 12, 13].

In addition to CDNs, Internet Exchange Points (IXPs) have been crucial in morphing the hierarchical structure of the AS internetwork, transforming it into a *flat* network [14]. The availability of IXPs is critical to CDNs, which prefer to have direct peering relationships with as many ASes as they can [15]. IXPs too are interested in hosting CDNs to provide a cost-effective way for the IXP members to reach content [16].

More recently, ASes have been slowly incorporating IPv6 reachability to deal with IPv4 address exhaustion. A set of milestones, such as IANA last IPv4 block transfer [17], The World IPv6 Launch [18] and ARIN IPv4 pool total depletion [19] have fostered IPv6 adoption. IPv6 is not backward compatible with IPv4, IPv4 and IPv6 paths between two end-hosts may differ [20].

In this paper we use the term "core" of the network to refer to the subset of ASes that are densely connected. In the past the "core" of the network mostly consisted of tier-1 networks, which were large international transit providers that were connected to all other tier-1 networks with peering links and had no transit providers of their own. CPs, as well as "eyeball" networks that were the destinations of traffic sourced by CPs were on the edge of the network. However, CPs and third-party CDNs have been building intercontinental backbone networks as well as making thousands of peering agreements in recent years. The growing significance of CPs has led to discussion and speculation about whether CPs are now the dominant players

in the Internet ecosystem [4].

Our goal is to investigate what role CPs now play in the Internet ecosystem, and in particular, if CPs are now a part of the "core" of the Internet. Specifically, we motivate this work with the following questions: How can we identify if a CP does or does not belong to the core of the Internet? If the core of the network does indeed include CPs, who are they?As the overall adoption of IPv6 has been slow, do we notice that delay on IPv4 and IPv6 core evolution? As the AS ecosystem has shown striking differences according to geographical regions [15], do we also see geographical differences in the role of CPs and their presence in the "core" of regional Internet structures? Finally, as more CPs deploy their private CDNs, can we detect "up and coming" CDNs that are not currently in the core of the network but are likely to be in the future?

We use the concept of *k-cores* to analyze the structure of the IPv4 AS-level internetwork over the last two decades. We first focus on seven large CPs, and confirm that they are all currently in the core of the Internet. We then dig deeper into the evolution of these large players to correlate observed topological characteristics with documented business practices which can explain when and why these networks entered the core. Next, we repeat the methodology but using IPv6 dataset to compare and contrast the evolution of CPs in both networks. Based on results, we investigate commercial and technical reasons why CPs started to roll out IPv6 connectivity.

We then take a broader view, characterizing the set of ASes in the core of the IPv4 Internet in terms of business type and geography. Our analysis reveals that an increasing number of CPs are now in the core of the Internet. Finally, we demonstrate that the k-core analysis has the potential to reveal the rise of "up and coming" CPs. To encourage reproducibility of our results, we make our datasets available via an interactive query system at `http://cnet.fi.uba.ar/TMA2018/`.

2. Related work

The increasing importance of CDNs in the Internet ecosystem has produced a vast literature on this topic, which shares some of the goals of the present article. Several articles studied the internal structure of CDNs [21, 22, 23, 24], where the focus was on the economic and technical benefits of CDNs, the need of data replication, techniques for content distribution and cache updates, and cache placement. CDN literature has also acknowledged the rising importance of private CDNs. Indeed, there have been several studies about the largest private CDNs. Google's CDN has been studied from many points of view: the growth of the serving infrastructure in recent years [25], QoE performance [26], internal load balancing [10], traffic engineering strategy run by its WAN SDN [9] and so on. Facebook's CDN was studied from the point of view of data replication [27], network administration [28], and Facebook's SDN [11]. Bottger *et al.* [29] studied the Netflix serving infrastructure, called Open Connect, due to its remarkably different architecture from other CDNs as well as the importance of Netflix in overall traffic share. Calder et al. analyzed Microsoft's CDN, known as Azure, as a representative example of an anycast CDN [30].

IXPs have also received a great deal of attention in the research and operational literature during the last decade. During the 2000s, IXPs were in part responsible for a *peering revolution*, offering neutral points for ASes to establish settlement-free peering agreements. IXPs encourage peering in order to keep traffic local and to avoid reaching local neighbors via either paid transit links or longer circuitous routes [3]. A well documented phenomenon is that the proliferation of IXPs has contributed to a *flattening* of the Internet [14], with hundreds of IXPs spread all over the world facilitating connectivity between thousands of co-located networks. In the research literature, a number of papers have studied the anatomy of large IXPs [6] as well as the role of IXPs in developing regions [31, 32].

Recently, Geoff Huston observed the wide-ranging effects of the flattening structure of the Internet and the rise of CPs [4]. Huston suggests that these trends are marginalizing the role of Transit Providers, terming this as *"The Death of Transit"*.

IPv6 has gained more attention in recent years due to the exhaustion of the IPv4 address space [17] and the increase of IPv6 adopters [33]. The growth of IPv6 reachability and its incompatibility with IPv4 have encouraged to study differences between both networks such as path lengths, performance and perspectives at the routing system [20].

The foreseeable long-time coexistence of both protocols, in addition to the already scarce number of unallocated IPv4 prefixes, have led to inter-organization IPv4 blocks purchase, allowed by some RIRs, know as the *Transfer market* [34, 35]. Despite the large number of transfers that have been signed since 2009, a peculiar pattern has been recently observed – Content Providers are purchasing large address blocks from American universities. This was evidenced when Google and Amazon got transferred IPv4 blocks that previously belonged to Merit (AS237) and MIT (AS3) [36, 37]. Averaging 10 dollars paid per address reinforces the importance that IPv4 still has over IPv6.

There is a vast body of previous literature on applying graph theoretic concepts to study the AS graph structure. Some examples of such work are papers that have introduced k-core decomposition to study properties of the network [38, 39, 40]. These works mainly take a mathematical perspective about the structure of the AS graph. In this work, we also utilize the k-core decomposition technique from graph theory to study the role specifically of CPs in the Internet over the years. However, we pair the graph-theoretic concept with domain knowledge, insights from other measurement datasets, and documented strategies and actions of the CPs themselves, which gives further

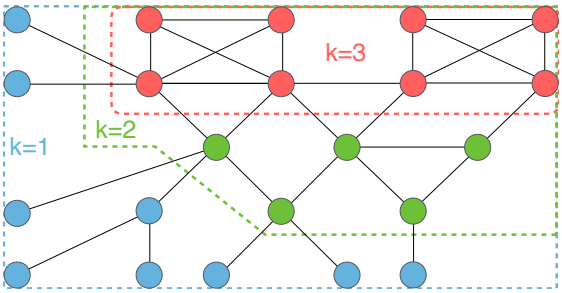


Figure 1: Example of a k-core decomposition of a given graph.

context and explanation for the observed phenomenon.

3. Methodology

Our goal is to study changes in the structure of the AS-level Internet ecosystem from the perspective of content providers and CDNs, specifically, whether large CPs are now part of the core of the network, and the historical evolution of when such a transition occurred. For this purpose, it is necessary to define a methodology to determine which ASes are part of the core of the network.

Since we look to prove that CPs have become as densely connected as Transit providers, the chosen methodology needs to determine AS connectivity based on the number of link of the AS and their neighbors as well. If the methodology is capable of doing so, and CPs are in fact as densely connected as Transit providers, values must be equal for both kind of ASes.

3.1. Definitions

To begin with, we examined a set of graph-theoretical metrics to determine which is capable indicating which ASes have the same level of connectivity. The studied metrics were node degree, Transit degree, Average nearest-neighbor degree (AND) and the k-core shell-index. The mathematical and computational complexity of these metrics is fairly different and the meaning of the metric as well.

Node degree. It is the simplest graph metric to evaluate the connectivity of a node. However, this metric does not take into account the properties of a node's neighbors. Furthermore, Faloutsos *et al.* [41] showed empirically that the node degree distribution of the AS-level ecosystem can be modeled using a random variable having a power-law distribution. With a power-law degree distribution, a non-negligible set of nodes will have large node degree while a large number of nodes will have much smaller degrees.

Transit degree. It is defined by the number of unique neighbors that appear on either side of an AS [42]. In other words, since the routing structure of the Internet is given by the AS-PATHS on BGP announcements, Transit degree counts in how many unique triples a node is, for all the observed AS-PATHS. Due to this definition, the Transit degree is a metric that measures the relevance of *intermediation* of an AS.

AND. As it is defined by Pastor-Satorras *et al.* [43], the AND is computed as the average degree of the neighbors of a AS. Compared to *Node degree*, this metric does take into account the relevance of the neighbors but it might be sensitive to the node degree distribution.

k-*core shell-index.* A k-core of a graph $\mathcal{G}$ is the maximum induced subgraph[1] in which all the vertices have at least degree k (see [44]). A vertex or node that belongs to a k-core has at least k neighbors which all have degree at least k. Moreover, a node that belongs to core k also belongs to any core $j < k$, thus the shell-index is given by the maximum core that a node belongs to. Figure 1 displays k-cores using a small graph example where nodes are colored to indicate their shell-index. As the figure shows, the shell-index (or simply "core") is given by the degree of the node as well as the degree of the neighbors in the induced graph. This can be seen in the example where some four-degree nodes are in core 2 while nodes of degree 3 are in core 3. Furthermore, AS graphs are *core-connected* [45], which means that there are k different paths between two ASes of the same k-core.

3.2. Evaluation on the AS ecosystem

Having defined a set of candidate metrics to determine which ASes are the most densely-connected in the Internet, we next analyze how these metrics perform. To do such analysis, we picked ASes that are presumably densely connected but have different business purpose. Among those ASes, we included the TOP10 ASes in CAIDA's AS-RANK [46] in March 2018, which are *TIER-1 Transit Providers* and seven popular Content Providers that corresponds to the top 7 *hypergiant* ASes identified by Bottger *et al.* [47]. Transit ASes are Level3 (AS3356), Telia (AS1299), NTT (AS2914), GTT (AS3257), Telecom Italia (AS6762), HE (AS6939), TATA (AS6453), PCCW (AS3491) and Level3 (formerly GBLX) (AS3549). The selected Content Providers are Akamai (AS20940), Amazon (AS16509), Apple (AS714), Facebook (AS32934), Google (AS15169), Netflix (AS2906) and Yahoo! (AS10310). For now on, we refer to the latter group as the *Big Seven*.

Table 1 displays the four metrics for the 17 ASes under study – 10 Transit ASes and 7 CPs, for the IPv4 AS graph. This table does not contain information about IPv6 because we just focus on analyzing what properties of the network these metric can capture rather than comparing results in IPv4 and IPv6 networks.

This table indicates that Node degree significantly varies among the TOP10 Transit ASes in the AS-RANK as well

[1] Let $G = (V, E)$ be any graph and W subset of vertices $W \subset V$. An *induced graph* is a subgraph of G whose nodes are given by W and its edges are the ones that have both endpoints in W.

	AS	ASN	AS Rank	Transit Degree	Degree	AND	K-Core
Transit ASes	Level 3 Comm.	3356	1	5130	4924	38	82
	Telia Company AB	1299	2	1972	2240	81	82
	Cogent Comm.	174	3	5718	6041	32	82
	NTT America	2914	4	2068	2438	75	82
	GTT Comm.	3257	5	1641	1577	86	81
	TELECOM ITALIA	6762	6	828	488	191	79
	Hurricane Electric, Inc.	6939	7	699	6792	53	82
	TATA Comm.	6453	8	2596	772	147	81
	PCCW Global, Inc	3491	9	352	636	186	81
	Level 3 Comm.	3549	10	1433	2648	33	72
Content Providers	Apple	714	5668	185	161	892	82
	Netflix	2906	4389	213	200	860	82
	Yahoo!	10310	687	278	291	621	82
	Google	15169	1397	237	205	834	82
	Amazon	16509	3054	173	203	900	82
	Akamai	20940	2679	285	364	563	82
	Facebook	32934	4417	227	202	905	82

Table 1: Transit degree, node degree, AND and k-core for the TOP10 ASes in the AS-RANK and seven well-known Content Providers in the IPv4 graph.Transit Degree and AS-RANK were taken from March 2018 snapshot which is different from the one in which we calculated the k-core decomposition and node degree, that was taken from October 2017. We assume these parameters did not vary significantly during that lapse.

as the *Big Seven*. For instance, while the observed node degree for Level3 (AS3356) is 4924 for Telecom Italia (AS6762) is 488. Moreover, node degree for CPs is by far smaller than for Transits since many peering links are often invisible in the dataset where these metrics were calculated [48].

Transit degree was meant to measure transit intermediation, therefore it is expected that Transit Providers have the highest Transit degree. Comparing both tables, Transit Degree for Transit ASes is usually an order of magnitude longer than for Content Providers. Content Providers are usually on the end of the AS-PATH, thus Transit Degree tends to be fairly small.

AND is fairly different between Transit and Content Provider ASes according Table 1. Graph edges between Transits and their customers are always visible. In addition, a large fraction of Transits customers are ASes that have a low node degree (1 or 2), thus AND tends to be low for Transit providers. On the other hand, Content Providers also peer with a large number of ASes of degree 1 or 2, however, those are links are likely to be peering links and would remain invisible in our dataset [48, 49]. Furthermore, CPs have no customers that affect their AND value. Therefore, CPs are just visible through a small subset of TIER-1 Transit providers, which lead CPs to have a fairly large AND value.

Table 1 shows that Large Content Providers as well as TIER-1 Transit Provider have the same (or almost the same) shell-index. Even though AND and k-core definitions are apparently similar, they are actually not. AND is defined by the average degree of the neighbors of a node while the shell-index of a node says that a node has k neighbors of degree k in the induced subgraph. Using k-cores we can see that CPs and TIER-1 are both densely connected because the ones on k=82 have al least 82 peers with ASes that have at least 82 peers with other networks. Thus, according to Table 1 , shell-index is the only indicator capable of reflecting connectivity equally for CPs and Transit providers.

3.3. Proposed methodology

To sum up the analysis of proposed metrics, the shell-index of the k-core decomposition is the only metric among the ones that we looked at that indicated similar values for Content Providers and Transit Providers. This is due to the definition of the k-core decomposition sets that an AS is densely-connected *if and only if* it is connected to ASes that are as connected as it is. This restriction is so strict that only large CPs and TIER-1 Transits can fulfill, and therefore we will use this definition to compute our analysis of the evolution of Content Providers. We are going to refer to the *core* of the network as the subset of ASes that are densely connected.

Applying the k-core decomposition, the central part of the network is made of ASes that belong to the maximum core k_{max}. In our analysis we study the evolution of cores of the CPs. However, the k_{max} as well as the k-indices of the AS graph change over time. For this reason, we normalize k in each snapshot by its k_{max} index, which leads to a normalized k with values between 0 and 1, referred to as k^*. For now on, TOPcore will refer to $k^* = 1$. To calculate k-core decomposition on each snapshot of an AS graph we used two tools, LaNet-vi [45], which also provides network visualization, and NetworkX, a python library.

4. Dataset

To apply the above k-core decomposition methodology on the Internet graph longitudinally, we need periodic historical snapshots of the IPv4 and IPv6 Internet's AS-level topology.

We rely on publicly available AS topology snapshots from CAIDA. CAIDA curates AS topology data from both BGP and traceroute-derived sources. The BGP AS relationship IPv4 dataset ([2]) is derived from BGP dumps taken from RouteViews and RIPE RIS collectors [42] from 1998 to present, and contains AS links observed at the BGP collectors along with an inferred business relationships. The BGP AS relationship IPv6 dataset [3] was created with exactly the same inputs but based on BGPv6 announcements [50] from 2004 to present.

We use a second IPv4 dataset which consists of AS links extracted from traceroutes from CAIDA's Archipelago (Ark) [51] vantage points towards every routed /24 prefix[4]. The two IPv4 datasets can provide somewhat different views of the Internet's AS-level topology. While the number of edges in each BGP data snapshot is larger than in traceroute data snapshots, traceroute often reveals peer-to-peer links which are not seen at BGP collectors [52]. To get the most complete picture of IPv4 AS-level connectivity, we chose to combine data from both the BGP and Ark datasets, which we refer to as the "Ark+BGP" dataset. This dataset consists of monthly snapshots dating from 1998 to present, which is sufficiently long to detect the evolution of the number of peers of CPs. Unfortunately, we did not have any similar traceroute-based dataset to enlarge the IPv6 BGP AS relationship dataset. To view the k-core decomposition using only the BGP dataset or traceroute dataset, we refer the reader to a website with these visualizations.[5]

A limitation of our methodology is that CPs also serve content from caches located within ISPs [12, 29], which are not visible as AS links in BGP or traceroute. Even CPs that follow an in-network caching strategy, however, generally need to peer in order to reach ISPs that are not willing to host caches in their networks, to fill the caches, and to serve dynamic content that cannot be cached. In this work we only study the evolution of AS-level connectivity of CPs; even though an analysis of cache infrastructure is important to shed some light about the way content is served, we consider such task out of the scope of this article and we will leave it to future work.

[2]CAIDA's BGP serial-1 dataset:`http://data.caida.org/datasets/as-relationships/serial-1/`

[3]CAIDA's BGP IPv6 AS-REL dataset:`http://data.caida.org/datasets/2015-asrank6-data-supplement/`

[4]The Ark dataset was merged with skitter dataset `http://data.caida.org/datasets/topology/skitter-aslinks/`.

[5]Graph visualization website:`http://cnet.fi.uba.ar/TMA2018/`.

5. A first look into the core evolution of CPs

A well-documented trend in the evolution of the Internet is that the set of ASes responsible for generating most of the traffic has been shrinking; recent studies have shown that only few tens of ASes together generate most of the traffic, while in the past that number was in the thousands [53, 1]. Given this trend toward traffic consolidation, we track the core evolution of seven big players, which we refer to as the *Big Seven*: Akamai (AS20940), Amazon (AS16509), Apple (AS714), Facebook (AS32934), Google (AS15169), Yahoo! (AS10310) and Netflix (AS2906). Our selection corresponds to the top 7 *hypergiant* ASes identified by Bottger *et al.* [47], where the authors ranked *hypergiants* based on port capacity, geographical footprint and traffic profile reported in PeeringDB.

Our *a priori* hypothesis is that all of these CPs currently belong to the TOPcore. We check whether our hypothesis is true, and if so, *when* and *how quickly* they reached the TOPcore. We then attempt to dig deeper into the reasons why we observe these CPs in the TOPcore, and correlate with external factors such as legal disputes, market expansions, QoE improvements, services releases etc. to explain why the CPs appeared in the TOPcore at a certain time.

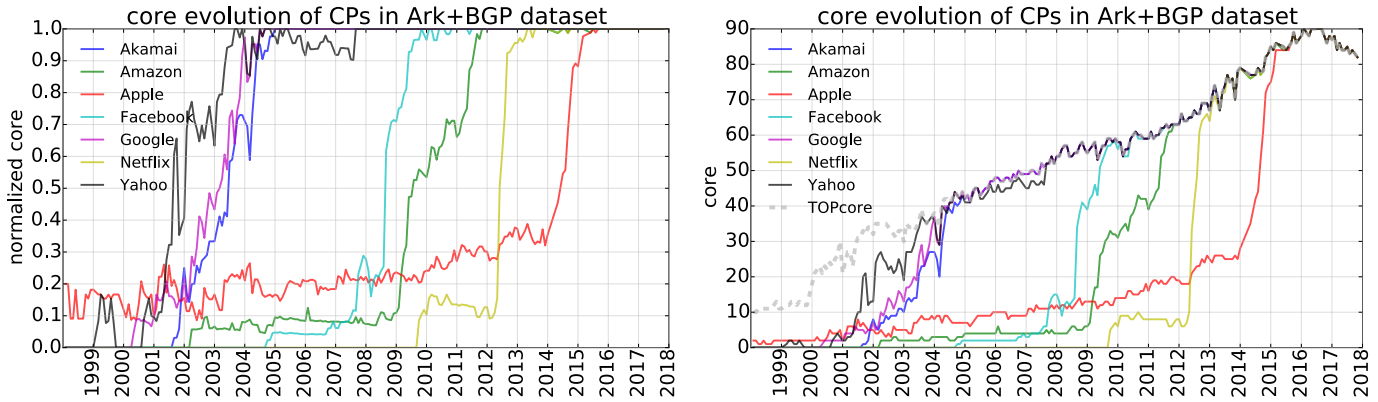
5.1. Looking at sibling ASes

Organizations, such as CPs, are likely to have multiple ASNs, where ASNs that belong to the same organization are usually called *siblings*. A wide variety of reasons is behind the fact of organizations having multiples ASNs, such as legacy ASN after merges or acquisitions, or having multiple ASNs for different purposes. However, organizations with multiple ASNs tend to have a *primary* ASN, which is presumably more visible than the rest.

We are interested in tracking the evolution of connectivity of Content Providers as organizations, thus we need to find all the ASNs that belong to each of the *Big Seven*. We looked for sibling ASes of the *Big Seven* using CAIDA's AS-to-organization list [54], which is a list based on WHOIS records that binds AS number with `org id`. First we looked for the `org ids` that corresponds to the well-known primary ASNs of the *Big Seven* and then we search all the ASNs that match with the previously obtained `org ids`.

After filtering, we found that 39 ASNs belong to exactly the same `org id` as the *Big Seven*, where Akamai has 17 ASNs, Apple 3, Amazon 3, Google 7, Facebook 2, Yahoo! 5 and Netflix 2. Among the siblings we found some ASNs which are popular and frequently mentioned by literature and operators, such as Google's AS36040 (formerly YouTube's ASN) and Apple's AS6185.

We tracked the evolution of the 39 ASNs over the years and we found that there have never been a sibling as relevant in terms of shell-index as the primary ASN in IPv4 graph. Whereas the primary ASNs do belong to the TOPcore, the secondary ASNs have been at most in cores halfway between core 1 and the TOPcore.



a) Normalized

b) Not normalized

Figure 2: k-core evolution of the *Big Seven* in IPv4 network. All of these CPs have reached the TOPcore.

After performing this analysis, we can conclude that for IPv4 it is efficient to only track the primary ASN of the *Big Seven*, and then correlate changes on those ASNs with business strategies.

5.2. Tracking the evolution of the Big Seven in IPv4

Figure 2 shows the monthly evolution of the CP-core on the Ark+BGP IPv4 dataset, where Figure 2a is normalized and Figure 2b is not. A first observation is that as of the end of 2017, all the studied CPs have joined the TOPcore, indicated by the fact that the normalized core value for each CP is 1.

There appear to be two groups among the studied CPs, one composed of Akamai, Google and Yahoo! which reached the TOPcore by 2005, and another comprising Amazon, Apple, Facebook and Netflix, which became members of the TOPcore between 2010 and 2015. The CPs in the first group are arguably more established, and have been providing a variety of online services for many years. The second group consists of CPs that at some point decided to deploy their own infrastructure and stop serving content using third-party CDNs such as Akamai, as multimedia content began to dominate the Internet traffic share [55]. Moreover, the transition from lower cores to upper cores among the members of the latter group is faster than in the former group. The fast evolution of Amazon, Apple, Facebook and Netflix cores is likely to have been encouraged by the vast number of peering facilities which appeared during the last decade [3, 56].

According to Figure 2b, the TOPcore has been always linearly growing, despite a small decay in late 2017. On the initial snapshot in 1999, there was no CP from the *Big Seven* in the TOPcore, and the maximum core was 10. The TOPcore reached its maximum during 2016, where the value of the core was 90. For example, in 2012 Netflix transitioned 71 cores (from core 6 to 77) to be able to reach the TOPcore. On the other hand, this may not be such a difficulty due to the expansion of peering infrastructure [14].

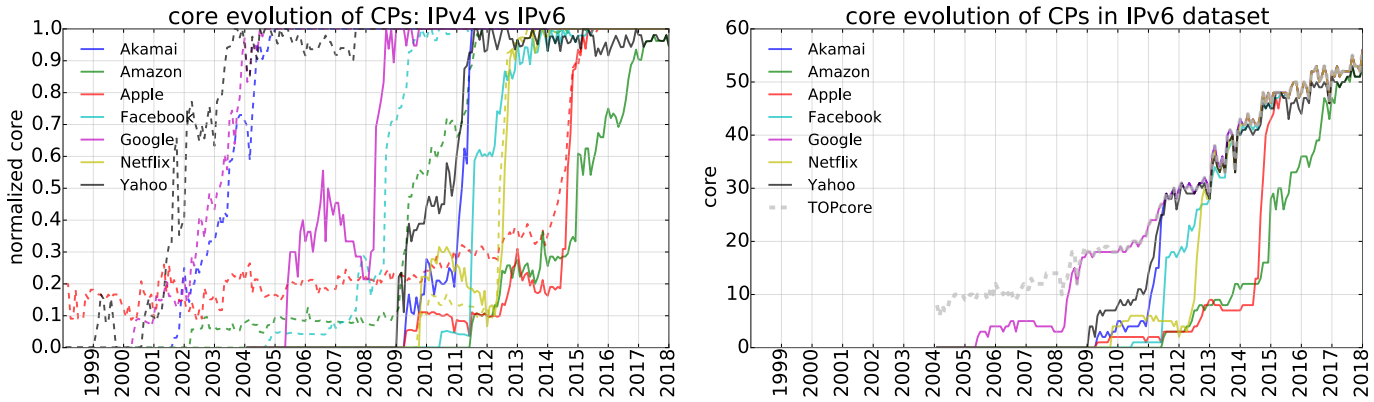
Next we dig deeper into the evolution of CPs individually. Specifically, we attempt to correlate the topological characteristics of the CPs (their core) with business strategies, acquisitions, or other factors which could explain why the CP entered the TOPcore.

Akamai. Akamai has been in the TOPcore since 2005. Akamai is a *pioneer* in content-delivery, and since its business model relies on providing high-availability low-latency hosting rather than generating content, they have always aimed to have a large number of peers.

Amazon. Amazon's infrastructure deployment appears to have occurred in two steps, according to Figure 2a, which is corroborated by publicly available information on Amazon's website [57]. In 2009, Amazon established its datacenter in Northern California, which coincides with the first growth. Between 2010 and 2012, Amazon established datacenters in several parts of the world, which coincides with the second growth spurt from 2010 to 2012.

Apple. We find that Apple's AS reached the TOPcore in 2015 after a quick growth. According to public information, Apple has been steadily offloading its content from Akamai onto its own CDN since 2013 [58]. Apple's traffic share has been growing rapidly in recent years due to software updates such as new OS releases [59] and security patches. Further, the company has recently announced that is planning to break into the TV market, producing original television shows, which will be served from Apple's CDN [60].

Facebook. Facebook's AS32934 got close to the TOPcore in 2010 after a rapid growth in its normalized core between 2008 and 2010. The number of users on Facebook grew exponentially from 12M in December 2006 to 350M by the end of 2009 [61] which coincides with Facebook's expansion



a) Normalized k-core evolutions of the *Big Seven*. Dashed lines display IPv4 while solid lines represent IPv6.

b) Not normalized

Figure 3: k-core evolution of the *Big Seven* in IPv6 network. All of these CPs have reached the TOPcore.

period and rise to the TOPcore. Although Facebook kept growing exponentially since then, the massive growth during that period encouraged Facebook to establish multiple peering agreements that enabled it to reach the TOPcore.

Google. Google was launched in September 1997 and in just a couple of years became the most popular search engine [62]. Over time, as Google started serving large volumes of video traffic via the acquisition of YouTube in 2006 [63], it expanded its CDN to get as close as possible to "eyeball" networks. Even before establishing its CDN, between 1999 and 2003, Google had peering agreements with tier-1 transit providers such as Level3 (AS3549), TATA (AS6453), Telstra (AS4637), NTT (AS2914), Zayo (AS6461), Qwest (AS209), GTT (AS3257) and Cogent (AS174). Links with a number of large Transit Providers resulted in Google becoming part of the same core level as those transit providers.

Yahoo!. The dot-com bubble in the early 2000s motivated Yahoo to build their own WAN infrastructure to avoid relying on transits for two reasons: i) to reduce content delivery dependency on intermediate networks between them and eyeball networks ii) to reduce operational costs [5]. In fact, Yahoo's core growth coincides with the end of the dot-com bubble in 2002.

Netflix. In 2012, it took Netflix less than a year to move from core $k^* = 0.1$ to the TOPcore. Netflix started offering video streaming in 2007 using third-party CDNs and transit providers. With the growing popularity of the service and increasing traffic volumes, the company moved content to its own Open Connect [64] platform in 2012, which is seen as a sharp increase in its normalized core value between 01/2012 and 09/2012 as shown in Figure 2a.

In summary, all of the studied CPs moved from third-party CDNs to private CDNs and entered the TOPcore. In particular, Apple, Facebook and Netflix all off-loaded content from Akamai. These changes led to significant loss of revenue for Akamai and a drop in its share price [65]. Despite losing major clients, Figure 2a shows that Akamai is still in the TOPcore, which means that Akamai's peering agreements do not depend exclusively on these large clients.

5.3. Tracking the evolution of the Big Seven in IPv6

Figure 3 shows the monthly evolution of the CP-core on the Ark+BGP IPv6 dataset, where Figure 3a is normalized and Figure 3b is not. Figure 3a also compares the normalized core evolution of the *Big Seven* in IPv4 and IPv6 cores. This figure confirms that all these ASes are currently present in both TOPcores, however, the date of arrival in the IPv6 TOPcore is significantly different than that in the IPv4 TOPcore. Two factors appear to have boosted the IPv6 adoption for theses companies: The World IPv6 Launch in 2012 [18] and ARIN's IPv4 pool depletion in 2015 [19].

Even though it has been several years since The World IPv6 Launch and the *Big Seven* reached the IPv6 TOPcore, the size of the IPv6 AS-level topology is still significantly smaller than IPv4 [66, 33]. As shown in Figures 2b and 3b, where the cores are not normalized, the maximum shell-index in the latest snapshot is 83 for IPv4 while it is 52 for IPv6.

Next, we look into the business strategies that fostered the *Big Seven* to rollout IPv6 connectivity.

Akamai. After a soft growth between 2009 and 2011, Akamai quickly reached the IPv6 TOPcore in 2011. This growth matches Akamai's recruiting campaign for early IPv6 adopters in 2011 [67], in which the company selected a subset of customers to start serving their content through dual-stack.

Amazon. Amazon's IPv6 rollout followed an almost identical trend to its IPv4 growth, but a few years delayed

as compared to IPv4. Amazon progressively incorporated countries where dual-stack services were available [68, 69], similar to its IPv4 worldwide expansion. A notable spurt in Amazon's IPv6 core growth occurred in late 2014. Examining the monthly snapshots from that time, Amazon started peering with a large number of Brazilian over IPv6 at the Brazilian IXP IX.br-SP.

Apple. Apple deployed its own CDN in 2015 and as seen in Figure 3a, both its IPv4 and IPv6 cores grew at the same pace. Just after Apple deployed its CDN, Apple started implementing IPv6 preference [70], which could be seen as an indicator of why Apple rolled out IPv6 reachability.

Google. This CP was the first among the *Big Seven* to reach the IPv6 TOPcore. Google started testing its IPv6 reachability using the domain `ipv6.google.com` during IETF72 in March 2008. Shortly after, in January 2009, Google became publicly available over IPv6 [71].

Facebook. Facebook reached the IPv6 TOPcore after two large steps, one in 2011 and the other in 2012. Facebook's IPv6 prefix `2a03:2880::/29` was, according to WHOIS records, allocated in August 2011. Then, Facebook was one of the participants of the World IPv6 Launch in June 2012 [72] and during this event the company reached the IPv6 TOPcore.

Yahoo!. The company has been endorsing IPv6 adoption, and it joined and sponsored IPv6 World Day and Launch in 2011 and 2012 respectively [18]. Yahoo! reached the IPv6 TOPcore a few months before IPv6 World Day in 2011.

Netflix. Netflix deployed its IPv4 and IPv6 CDN (called Open Connect) simultaneously in 2012. As shown in Figure 3a, Netflix rapidly climbed in both cores at the same pace. Although the maximum core on IPv4 and IPv6 were different in 2012 (Figures 2b and 3b), Netflix's aggressive peering strategy allowed them to become densely-connected in both cores at the same time. Moreover, according to Netflix information, video is delivered over IPv6 whenever possible [73, 74].

6. Evolution by geographical region of the IPv4 core

We also investigate in whether CPs belong to the IPv4 TOPcore in each geographical region, defined as the Regional Internet Registries (RIR) regions. We repeat the analysis of speed and date of arrival done in Section 5.2 for each CP in every RIR with a focus on detecting differences by region, especially systematic delays in when certain CPs appeared in specific regions.

To determine which regions an AS is present in, we use the NetAcuity [75] geolocation database to geolocate each prefix advertised by an AS in a given snapshot. For this analysis we will just focus on IPv4 core evolution due to the lack of geolocation entries for IPv6 analysis. The (in)accuracy of geolocation databases has been studied extensively [76]. However, previous work has found that the NetAcuity database is mostly reliable for country-level geolocation [77]. We use RIR-level granularity in this work, so we believe that this analysis is not affected by inaccuracies in geolocation. After geolocating ASes, we combine the monthly "Ark+BGP" snapshots with the mapping between AS and RIR to create monthly RIR subgraphs.

There are two issues with this basic methodology that we need to account for. First, we need AS geolocation information throughout the duration of "Ark+BGP" dataset. However, CAIDA only had NetAcuity records since November 2011, while our topology dataset starts in January 1998. Second, NetAcuity appears to incur a time lag between when a prefix is active in a new location and when it appears at that location in the database. For example, NetAcuity started reporting the presence of Netflix in the LACNIC region in December 2016, while a June 2015 Wayback Machine snapshot [6] already showed Netflix as a member of a Brazilian IXP. As our goal is to track historical evolution, it is necessary to include an AS in the RIR subgraph when changes are actually happening and not once they have already happened. To account for these issues we made two modifications to the basic methodology.

1. We assume that the 7 CPs we study have always had a presence in every RIR. While building the RIR subgraph, however, we only include observed connectivity between the CPs and other ASes geolocated to the RIR.
2. We assume that prior to November 2011 (the start of our Netacuity dataset), ASes had the same locations that they had in November 2011.

While this methodology allows us to create RIR subgraphs, we cannot infer where the connection between two ASes actually happens when those ASes have presence in multiple RIR subgraphs. For instance, Google and Level3, which are currently present in every RIR subgraph, may not have a physical link in each RIR.

6.1. Geographical evolution of the Big Seven in IPv4

Figure 4 shows the evolution of each CP by RIR. We find that all CPs have reached the IPv4 TOPcore in every RIR although the arrival date varies by CP and RIR.

Amazon and Facebook show differences between RIRs in their growth in the late 2000s and early 2010s. Amazon first established datacenters and PoPs in the US before 2009, then expanded to Singapore (APNIC) in 2010,

[6] Wayback Machine snapshot of members of Brazilian IXP. 06/2015:`http://web.archive.org/web/20150617231252/http://ix.br/particip/sp`

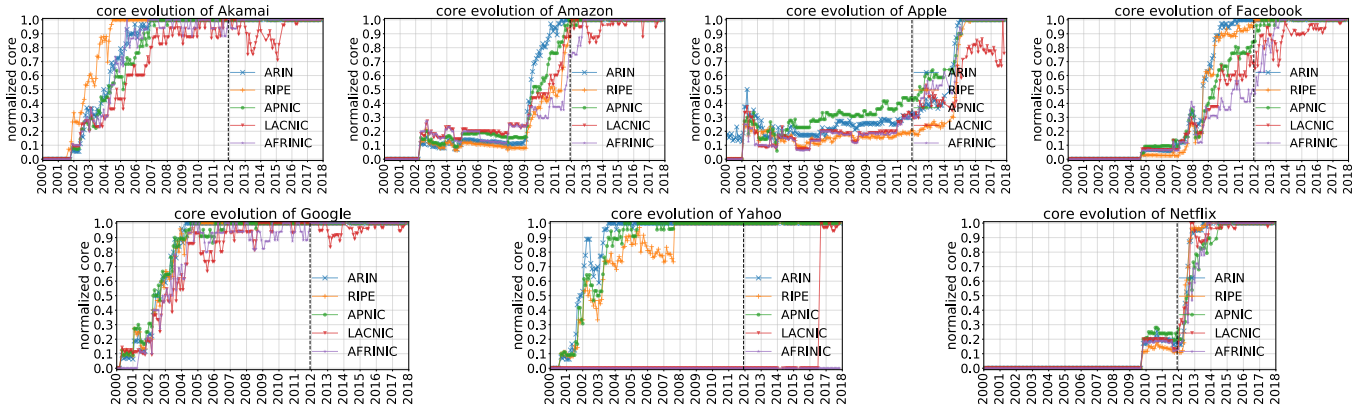


Figure 4: k-core evolution of the *Big Seven* in each RIR. The dashed line displays the beginning of NetAcuity geolocation database.

Brazil (LACNIC) in 2011, and several locations in Europe (RIPE) in 2011 [57]. Figure 4 shows that Amazon's core trends follow its documented infrastructure deployment. Facebook, which has been part of the worldwide IPv4 TOPcore since 2009, lagged in APNIC, LACNIC and AFRINIC, where it got to the TOPcore several years after ARIN and RIPE. Facebook got to the IPv4 TOPcore in ARIN in August 2010, APNIC in August 2012, LACNIC in August 2013 and in AFRINIC in March 2013. In RIPE, Facebook has been in the upper cores ($k^* \geq 0.9$) since early 2010, however, it finally reached the IPv4 TOPcore in January 2012. Facebook publicly acknowledged its lack of presence in developing regions and took steps to correct in order to improve user QoE in those regions [78].

Since the *Big Seven* are all U.S. based companies, one might expect that they first reached the IPv4 TOPcore in ARIN, and later expanded to developing regions such as LACNIC and AFRINIC. We investigate this hypothesis next, while noting that the analysis that follows is specific to these companies and may not generalize to other content providers or regions. Figure 4 shows, however, that Akamai and Google showed negligible differences across RIRs in the early 2000s, which does not match documented information about their CDN deployment. For instance, Google established a PoP in Argentina only in 2011 [79]. The reason for this discrepancy is that Akamai and Google had peering links with tier-1 transit providers present in those regions, which caused the CPs to be in the TOPcore of those regions as well. A look at peering relationships in the early 2000s confirms this hypothesis — Google was not present in the LACNIC region, however, it peered with Level3 (AS3549), TATA (AS6453) and Qwest (AS209), which were present in LACNIC. We confirmed that the tier-1 ASes were present in LACNIC because they peered with the two largest Argentinian ISPs, Cablevision (AS10318) and TASA (AS4926), which were only present in Argentina at the time.

Similar Google and Akamai, Yahoo had similar core evolution trends in ARIN, RIPE and APNIC in early 2000s. However, Yahoo had a significant delay in LACNIC region

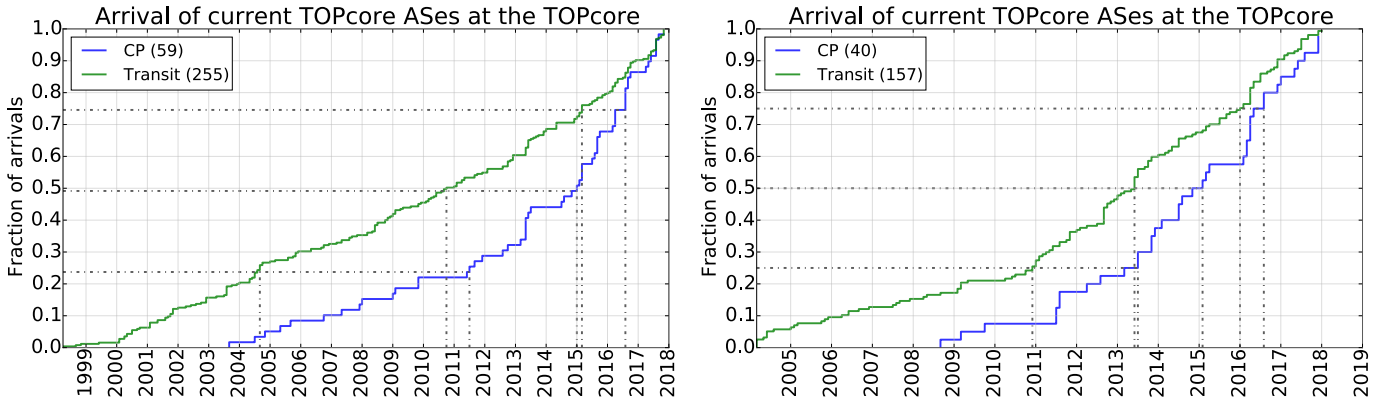
Table 2: Percentage of local peers in each region.

	%	ARIN	RIPE	APNIC	LACNIC	AFRINIC
Akamai	2007	0.33	0.75	0.21	0.0	0.05
	2012	0.45	0.74	**0.45**	0.11	0.0
	2017	0.41	0.71	0.47	**0.56**	**0.23**
Amazon	2007	1.0	0	0	0	0
	2012	*0.49*	**0.75**	**0.24**	**0.35**	0.0
	2017	0.40	0.68	0.37	0.53	0.03
Apple	2007	0.73	0	0.40	0	0
	2012	0.60	0.15	0.29	0	0
	2017	*0.42*	**0.67**	0.4	**0.17**	**0.07**
FB	2007	0.51	0.68	0.21	0.11	0.11
	2012	0.49	0.75	0.37	**0.36**	0.05
	2017	0.44	0.73	0.37	0.51	**0.14**
Google	2007	1.0	0	0	0	0
	2012	*0.43*	**0.81**	0.27	0.07	0.0
	2017	0.39	0.70	**0.38**	**0.56**	**0.07**
Yahoo!	2007	0.7	0.45	0.15	0	0
	2012	0.57	0.72	0.44	0	0
	2017	0.53	0.73	0.46	**0.6**	0
Netflix	2007	0	0	0	0	0
	2012	**0.86**	0.14	0	0	0
	2017	*0.39*	**0.77**	**0.39**	**0.57**	**0.10**

where the company reached the TOPcore in 2016 when it joined the Brazilian IXP in Sao Paulo [7]

Netflix and Apple were the latest to enter the worldwide IPv4 TOPcore as well as the IPv4 TOPcore of each RIR. Netflix was in the lower cores ($k^* < 0.3$) in every RIR in January 2012. By January 2014 it moved to the IPv4 TOPcore in every RIR. Apple's growth was similar — in

[7] Wayback Machine snapshot of members of Brazilian IXP. 09/2016`http://web.archive.org/web/20160904012004/http://ix.br/particip/sp`



a) IPv4 b) IPv6

Figure 5: Date of first arrival at the TOPcore for ASes which currently compose the TOPcore.

Table 3: Origin according to WHOIS for TOPcore ASes

		ARIN	RIPE	APNIC	LACNIC	AFRINIC	Unknown
COREv4	Content	36	20	3	0	0	-
	Transit	35	165	38	3	8	6
COREv6	Content	25	14	1	0	0	-
	Transit	20	108	15	3	6	7

June 2014 it was in cores lower than 0.5. One year later it was in the IPv4 TOPcore of every RIR except LACNIC where it reached the TOPcore in Jan 2017.

6.2. Local Peers

The analysis of the previous section showed that core evolution does not necessarily reflect the geographical expansion of CPs. Here we present a complementary analysis. Table 2 shows the percentage of peers of a CP in a region that are registered in that region (according to WHOIS records). For example, Google had 38% of local peers in APNIC in 2017, meaning that 38% of Google's links with ASes present in APNIC were with ASes registered in APNIC, while the remaining 62% were with ASes present in APNIC but registered elsewhere. This metric provides information about when a CP first arrived in a region, as that would intuitively lead to an increase in the local peering metric.

Table 2 shows that Akamai, Google and Yahoo! significantly increased the number of local peers in Latin America (LACNIC) in the last five years. APNIC has also shown a growth in the number of local peers, but slower than in LACNIC. In contrast to Figure 4 where all of the CPs belong to every TOPcore, Table 2 shows a fairly low number of local peers of these CPs in AFRINIC. As of 2017, Akamai had the largest fraction with 0.23, Facebook second with 0.14 and all the rest were under 0.10.

While the percentage of local peers of CPs increases over the years in regions where they initially had a small fraction of local peers, ARIN shows the opposite trend. This is likely because the studied CPs are U.S. companies. Consequently, their number of local peers in ARIN saturates, while the number of non-local peers increases as companies outside the U.S. deploy infrastructure in ARIN and peer with the CPs.

7. The TOPcore beyond the Big Seven

We conclude our analysis by looking at other networks in the TOPcore. Specifically, we investigate four aspects related to this set of ASes: i) Composition of the TOPcores ii) Evolution of Dual-Stack adopters iii) Time required to reach the TOPcore iv) Trends of some other remarkable CPs that were not included in the *Big Seven*.

To identify ASes in the TOPcore, we use the criterion that an AS must be in $k^* > 0.975$ at any point in time, and in $k^* \geq 0.95$ during the last six months of our dataset (Mar-2017 to Oct-2017). Note that this definition of the TOPcore is broader than that used in the previous section where the criterion for belonging to the TOPcore was $k^* = 1$.

7.1. Composition of the TOPcores

We would like to investigate how many networks are in the TOPcore, what type of networks they are (transit or content), and what fraction of the TOPcore networks is accounted for by content networks.

By the TOPcore definition, we had 314 ASes in the IPv4 TOPcore — 59 Content Providers and 255 Transit/Access Providers according to CAIDA's AS classification [80]. In the IPv6 TOPcore we found 197 ASes, where 40 are Content Providers and 157 Transit/Access providers. We refer to the set of ASes in IPv4 and IPv6 TOPcore as COREv4 and COREv6, respectively.

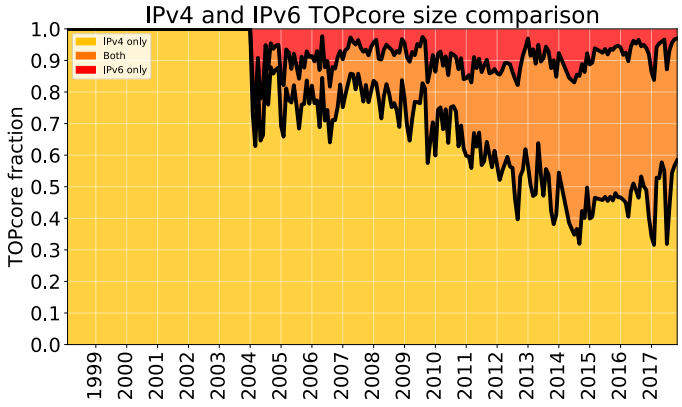


Figure 6: Evolution of dual-stack ASes among members of both TOPcores.

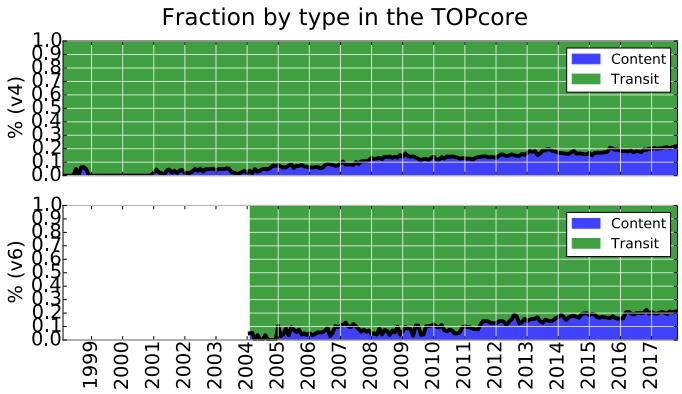


Figure 7: Monthly evolution of the fraction of CPs and Transit in the TOPcore.

Figure 5a shows the fraction of COREv4 (separated into Content and Transit) that first reached the IPv4 TOPcore over time. This plot clearly shows that over time, more CPs have been joining the TOPcore. Interestingly, 75% of the CPs in the studied set first entered the TOPcore after 2011. Moreover, we see two distinct phases in the CP curve — the rate at which CPs arrived in the TOPcore has increased since 2011. The arrival of Transit Providers, on the other hand, appears steady over the years.

Figure 5b displays the same analysis as in Figure 5a but for the IPv6 TOPcore. While the trend for Transits in Figure 5a linearly increased during the years, Figure 5b shows an inflection point in early 2011 when IANA announced the allocation of its last /8 to the RIR [17]. With respect to Content Providers, 75% of CPs in COREv4 reached TOPcore after 2011, while more than 90% of CPs in COREv6 reached the TOPcore in the same period. The arrival of Transit and Content in the IPv6 TOPcore show an acceleration, especially for CPs, after ARIN announced its IPv4 pool reached zero in September 2015 [19].

Table 3 shows the geographical distribution of ASes in the TOPcores. We see that CPs in COREv4 and COREv6 are mostly from ARIN and RIPE (with the exception of 3 and 1 from APNIC in COREv4 and COREv6 respectively). However, among Transit Providers, RIPE has significantly more ASes in COREv4 as well as COREv6 than other regions. AFRINIC and LACNIC have negligible or no presence in either category. APNIC has a considerable number of Transit Providers in COREv4 and COREv6 but few CPs. Comparing the geographical composition of in COREv4 and COREv6 by category, both have exactly the same distribution. Therefore, the geographical distribution of densely-connected ASes is invariant to changes on the IP protocol.

7.2. Dual-stack in the TOPcore

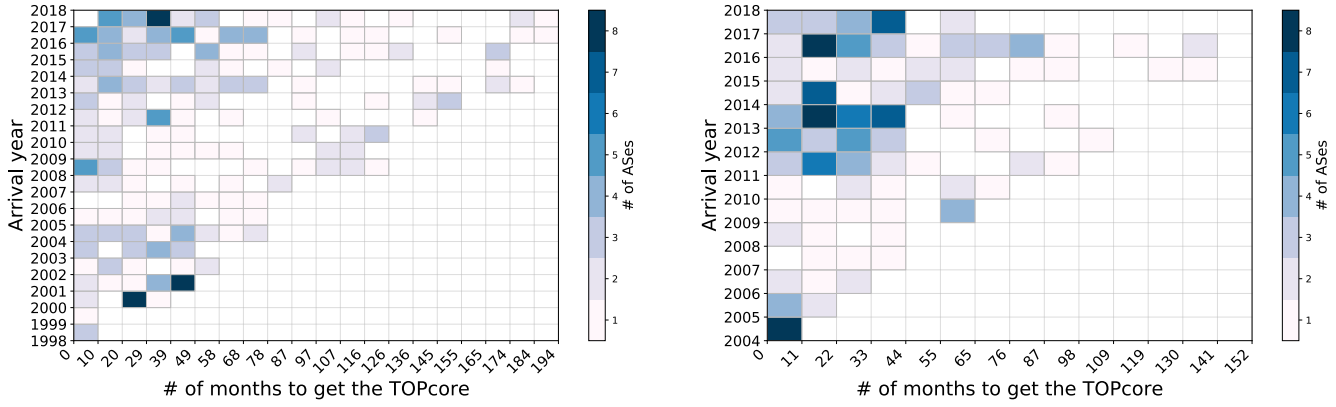
Next, we analyze the fraction of ASes that belong simultaneously to both TOPcores in each snapshot since 1999. Figure 6 displays the fraction of ASes in the IPv4 TOPcore, IPv6 TOPcore and in both. Since 2004 when IPv6 data starts, the fraction of ASes that only belong to the IPv6 TOPcore has been fluctuating around 10%. However, since then more and more ASes have been incorporating dual stack technology, which is reflected on the increase of ASes that belong to both TOPcores and the reduction of member that exclusively belong to the IPv4 TOPcore. In March 2018, the network indicates that roughly 50% the TOPcore ASes are reachable via IPv6. This figure lets us conclude that densely-connected ASes, which already are in the IPv4 TOPcore, are rolling out IPv6 but it is fairly rarely to find ASes that only belong to the IPv6 TOPcore.

We next investigate the composition of ASes in the TOPcore over time. In Figure 7, we applied the TOPcore criterion to determine which ASes belong to the TOPcore every month, and then classified the ASes in the TOPcore as Content or Transit. We find that the fraction of CPs in both TOPcores has been steadily increasing; as of the October 2017 snapshot, 22% of ASes in both TOPcores were CPs. Note that the absolute number of ASes in the TOPcores has been increasing as well, which implies that both TOPcores have been incorporating more CPs than Transit ASes over time.

7.3. Speed to reach the TOPcore

We are interested in analyzing *how quickly* networks reached the TOPcore.

Figures 8a and 8b show a heatmap of the number of ASes that arrived at the TOPcore at a certain time and at a certain *speed*. We define *speed* as the number of months to move from $k^* = 0.3$ to $k^* = 0.975$, and this definition is based on the transitions from lower to upper cores seen in Figure 2a. Figure 8a shows that 172 ASes from COREv4 joined the TOPcore between 2011 and 2018 and most of them moved from lower cores in just a few months, where the average time required for joining COREv4 was 61 months. Figure 8b shows the counterpart for IPv6 where 154 ASes from COREv6 joined the TOPcore between 2011 and 2018. The average time required for transitioning from lower cores to the TOPcore in IPv6 was on



a) IPv4 b) IPv6

Figure 8: Correlation between speed of growth and date of arrival at the TOPcore.

average 35 months, which is smaller than IPv4 network. This fast evolution of the IPv4 TOPcore in recent years can be possibly explained by the growth of the number of peering facilities and participants at those facilities in this time frame.

7.4. Other remarkable CPs in the TOPcore

Finally, we study the core evolution of nine other remarkable CPs that belong to the TOPcore but were not included in the *Big Seven*. Seven of the nine selected ASes are the remaining ASes in Bottger *et al.*'s [47] TOP15 list, except Hurricane Electric (AS6939) which we do not consider as a CP since it is labeled as Transit/Access in CAIDA's AS classification [80]. These seven ASes are OVH (AS16276), LimeLight (AS22822), Microsoft (AS8075), Twitter (AS13414), Twitch (AS46489), CloudFlare (AS13335) and EdgeCast (AS15133). The other two ASes are Booking.com (AS43996) and Spotify (AS8403). Interestingly, Booking.com or Spotify are not normally considered among the top CPs, however, they are in both TOPcores.

Figures 9a and 9b show the evolution of nine CPs that have joined the IPv4 and IPv6 TOPcores in recent years (different from the Big Seven). The figures also indicate that many rapidly transitioned from lower to upper cores.

Twitch is another remarkable CP in this list, which may not be as known as the *Big Seven* are, however, it is extremely popular among the gamer community. Twitch is a video streaming platform that allows its users to live stream what they are currently playing. The service is responsible for being the fourth traffic source of peak traffic in the US [81] and its audience is even larger than traditional media broadcasters [82]. Live streaming video is exclusively served by Twitch serving infrastructure (AS46489) that spreads over 21 airport codes and 12 countries [83]. Furthermore, looking at Twitch's records in PeeringDB, the CP peers at 47 IXPs all over the world [84]. Twitch's IPv4 CDN deployment is clearly evidenced in Figure 9a, where it rapidly reached the TOPcore in 2014. Twitch is also present in COREv6 as shown in Figure 9b. It is worth noting that according to this figure, Twitch IPv6 rollout happened in 2017.

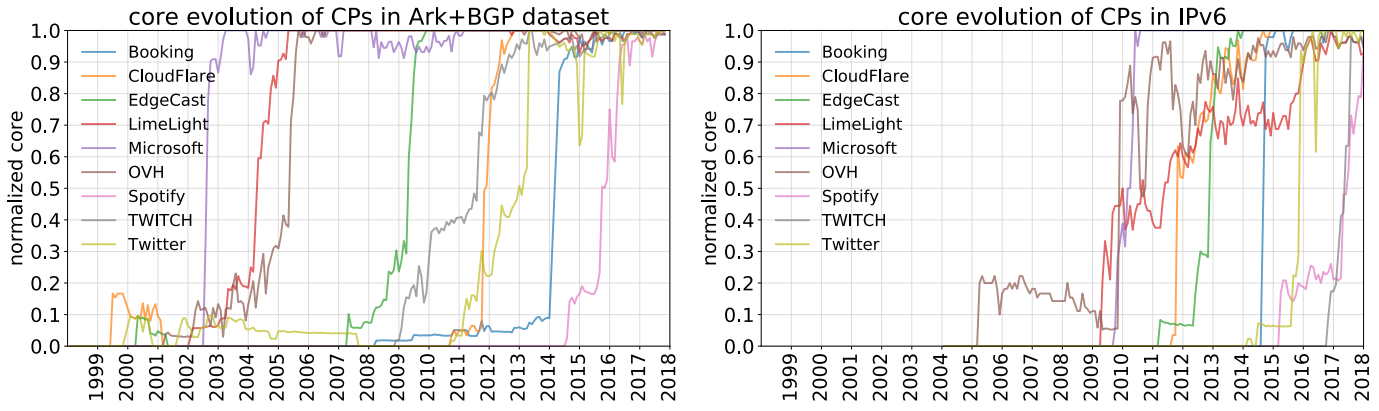
We found trends similar trends in Figure 9 and Figure 3a (*Big Seven*). To begin with, ASes that reached the IPv4 TOPcore in early 2000s, such as LimeLight in Figure 9 or Akamai in Figure 3a, postponed IPv6 rollout. On the other hand, we also notice ASes that deployed their CDN in recent years are the ones that have less or no delay between the IPv4 and IPv6 core evolution. While Netflix evidences this pattern in Figure 3a, so does Booking.com in Figure 9.

8. Conclusions

In this work we demonstrated that CPs have taken a decisive role in the AS ecosystem, where seven large companies in the Internet content market have moved towards the core of the network. By analyzing the evolution of the cores of the CPs, we were able to identify possible reasons related to business practices, strategies, and geographical expansion that explain the rise of these networks to the top core. Furthermore, we showed the core of the network has been rapidly incorporating content ASes over time.

We also showed that most of the CPs as well as Transits reached the IPv6 TOPcore several years after reaching IPv4 TOPcore, which coincides with the fact that many ASes postponed IPv6 rollout. However, ASes were faster to reach IPv6 TOPcore since the physical infrastructure was already available by then.

We believe that analysis of core evolution can be a possible tool to identify ASes that are increasing in significance, the so-called "up and coming" CPs. We refer the reader to the following website to replicate our results: `http://cnet.fi.uba.ar/TMA2018/`



a) IPv4 b) IPv6

Figure 9: k-core evolution of CPs other than the *Big Seven*.

9. Acknowledgments

This work was partially founded by UBACyT 2014 (20020130200122BA) and NSF grant CNS-1513847. Esteban Carisimo acknowledges CONICET Argentina for a PhD fellowship.

References

[1] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, F. Jahanian, Internet inter-domain traffic, in: Proceedings of the ACM SIGCOMM 2010 Conference, SIGCOMM '10, ACM, New York, NY, USA, 2010, pp. 75–86. doi:10.1145/1851182.1851194.
URL http://doi.acm.org/10.1145/1851182.1851194

[2] k. claffy, G. Polyzos, H. Braun, Traffic characteristics of the T1 NSFNET backbone, in: IEEE Conference on Computer Communications (INFOCOM), Vol. 2, 1993, pp. 885–893.

[3] N. Chatzis, G. Smaragdakis, A. Feldmann, W. Willinger, There is more to ixps than meets the eye, SIGCOMM Comput. Commun. Rev. 43 (5) (2013) 19–28. doi:10.1145/2541468.2541473.
URL http://doi.acm.org/10.1145/2541468.2541473

[4] G. Huston, The death of Transit, https://blog.apnic.net/2016/10/28/the-death-of-transit/ (2016).

[5] P. Gill, M. Arlitt, Z. Li, A. Mahanti, The flattening internet topology: Natural evolution, unsightly barnacles or contrived collapse?, in: M. Claypool, S. Uhlig (Eds.), Passive and Active Network Measurement, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 1–10.

[6] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, W. Willinger, Anatomy of a large european ixp, in: Proceedings of the ACM SIGCOMM 2012 Conference, SIGCOMM '12, ACM, New York, NY, USA, 2012, pp. 163–174. doi:10.1145/2342356.2342393.
URL http://doi.acm.org/10.1145/2342356.2342393

[7] T. Leighton, Improving performance on the internet, Commun. ACM 52 (2) (2009) 44–51. doi:10.1145/1461928.1461944.
URL http://doi.acm.org/10.1145/1461928.1461944

[8] Wired, Google and Netflix Make Land Grab On Edge Of Internet, https://www.wired.com/2012/06/cdn/ (2016).

[9] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hölzle, S. Stuart, A. Vahdat, B4: Experience with a globally-deployed software defined wan, in: Proceedings of the ACM SIGCOMM 2013 Conference, SIGCOMM '13, ACM, New York, NY, USA, 2013, pp. 3–14. doi:10.1145/2486001.2486019.
URL http://doi.acm.org/10.1145/2486001.2486019

[10] D. E. Eisenbud, C. Yi, C. Contavalli, C. Smith, R. Kononov, E. Mann-Hielscher, A. Cilingiroglu, B. Cheyney, W. Shang, J. D. Hosein, Maglev: A fast and reliable software network load balancer, in: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), USENIX Association, Santa Clara, CA, 2016, pp. 523–535.
URL https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eisenbud

[11] B. Schlinker, H. Kim, T. Cui, E. Katz-Bassett, H. V. Madhyastha, I. Cunha, J. Quinn, S. Hasan, P. Lapukhov, H. Zeng, Engineering egress with edge fabric: Steering oceans of content to the world, in: Proceedings of the ACM SIGCOMM 2017 Conference, SIGCOMM '17, ACM, New York, NY, USA, 2017, pp. 418–431. doi:10.1145/3098822.3098853.
URL http://doi.acm.org/10.1145/3098822.3098853

[12] A.-J. Su, D. R. Choffnes, A. Kuzmanovic, F. E. Bustamante, Drafting behind akamai: Inferring network conditions based on cdn redirections, IEEE/ACM Trans. Netw. 17 (6) (2009) 1752–1765. doi:10.1109/TNET.2009.2022157.
URL http://dx.doi.org/10.1109/TNET.2009.2022157

[13] N. Economides, J. Tåg, Network neutrality on the internet: A two-sided market analysis, Information Economics and Policy 24 (2) (2012) 91–104.

[14] A. Dhamdhere, C. Dovrolis, The internet is flat: Modeling the transition from a transit hierarchy to a peering mesh, in: Proceedings of Conference on emerging Networking EXperiments and Technologies, CoNEXT '10, ACM, New York, NY, USA, 2010, pp. 21:1–21:12. doi:10.1145/1921168.1921196.
URL http://doi.acm.org/10.1145/1921168.1921196

[15] A. Dhamdhere, C. Dovrolis, Ten years in the evolution of the internet ecosystem, in: Proceedings of the 2008 Internet Measurement Conference, IMC '08, ACM, New York, NY, USA, 2008, pp. 183–196. doi:10.1145/1452520.1452543.
URL http://doi.acm.org/10.1145/1452520.1452543

[16] P. Faratin, Economics of overlay networks: An industrial organization perspective on network economics, in: Proceedings of the NetEcon+ IBC workshop, 2007, p. 1.

[17] IANA, The IANA IPv4 Address Free Pool is Now Depleted, https://www.arin.net/vault/announcements/2011/20110203.html (2011).

[18] Internet Society, World IPv6 Launch , www.worldipv6launch.org/ (2012).

[19] ARIN, ARIN IPv4 Free Pool Reaches Zero , https://www.arin.net/vault/announcements/2015/20150924.html. (2015).

[20] A. Dhamdhere, M. Luckie, B. Huffaker, k. claffy, A. Elmokashfi, E. Aben, Measuring the deployment of ipv6: Topology, routing and performance, in: Proceedings of the 2012 Internet Measurement Conference, IMC '12, ACM, New York, NY, USA, 2012,

pp. 537–550. doi:10.1145/2398776.2398832.
URL http://doi.acm.org/10.1145/2398776.2398832

[21] J. Dilley, B. Maggs, J. Parikh, H. Prokop, R. Sitaraman, B. Weihl, Globally distributed content delivery, IEEE Internet Computing 6 (5) (2002) 50–58. doi:10.1109/MIC.2002.1036038.
URL https://doi.org/10.1109/MIC.2002.1036038

[22] G. Pallis, A. Vakali, Insight and perspectives for content delivery networks, Commun. ACM 49 (1) (2006) 101–106. doi:10.1145/1107458.1107462.
URL http://doi.acm.org/10.1145/1107458.1107462

[23] C. Huang, A. Wang, J. Li, K. W. Ross, Understanding hybrid cdn-p2p: Why limelight needs its own red swoosh, in: Proceedings of the 18th International Workshop on Network and Operating Systems Support for Digital Audio and Video, NOSSDAV '08, ACM, New York, NY, USA, 2008, pp. 75–80. doi:10.1145/1496046.1496064.
URL http://doi.acm.org/10.1145/1496046.1496064

[24] M. Pathan, R. Buyya, A. Vakali, Content delivery networks: State of the art, insights, and imperatives, Content Delivery Networks (2008) 3–32.

[25] M. Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, R. Govindan, Mapping the expansion of google's serving infrastructure, in: Proceedings of the 2013 Internet Measurement Conference, IMC '13, ACM, New York, NY, USA, 2013, pp. 313–326. doi:10.1145/2504730.2504754.
URL http://doi.acm.org/10.1145/2504730.2504754

[26] P. Casas, A. D'Alconzo, P. Fiadino, A. Br, A. Finamore, T. Zseby, When youtube does not work?analysis of qoe-relevant degradation in google cdn traffic, IEEE Transactions on Network and Service Management 11 (4) (2014) 441–457. doi:10.1109/TNSM.2014.2377691.

[27] Q. Huang, K. Birman, R. van Renesse, W. Lloyd, S. Kumar, H. C. Li, An analysis of facebook photo caching, in: Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles, SOSP '13, ACM, New York, NY, USA, 2013, pp. 167–181. doi:10.1145/2517349.2522722.
URL http://doi.acm.org/10.1145/2517349.2522722

[28] Y.-W. E. Sung, X. Tie, S. H. Wong, H. Zeng, Robotron: Top-down network management at facebook scale, in: Proceedings of the 2016 ACM SIGCOMM Conference, SIGCOMM '16, ACM, New York, NY, USA, 2016, pp. 426–439. doi:10.1145/2934872.2934874.
URL http://doi.acm.org/10.1145/2934872.2934874

[29] T. Böttger, F. Cuadrado, G. Tyson, I. Castro, S. Uhlig, Open connect everywhere: A glimpse at the internet ecosystem through the lens of the netflix cdn, SIGCOMM Comput. Commun. Rev. 48 (1) (2018) 28–34. doi:10.1145/3211852.3211857.
URL http://doi.acm.org/10.1145/3211852.3211857

[30] M. Calder, A. Flavel, E. Katz-Bassett, R. Mahajan, J. Padhye, Analyzing the performance of an anycast cdn, in: Proceedings of the 2015 Internet Measurement Conference, IMC '15, ACM, New York, NY, USA, 2015, pp. 531–537. doi:10.1145/2815675.2815717.
URL http://doi.acm.org/10.1145/2815675.2815717

[31] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, E. Katz-Bassett, Peering at the internet's frontier: A first look at isp interconnectivity in africa, in: M. Faloutsos, A. Kuzmanovic (Eds.), Passive and Active Measurement, Springer International Publishing, Cham, 2014, pp. 204–213.

[32] R. Fanou, P. Francois, E. Aben, On the diversity of interdomain routing in africa, in: J. Mirkovic, Y. Liu (Eds.), Passive and Active Measurement, Springer International Publishing, Cham, 2015, pp. 41–54.

[33] Geoff Huston, What Drives IPv6 Deployment?, https://labs.ripe.net/Members/gih/what-drives-ipv6-deployment (2018).

[34] I. Livadariu, A. Elmokashfi, A. Dhamdhere, k. claffy, A first look at ipv4 transfer markets, in: Proceedings of Conference on emerging Networking EXperiments and Technologies, CoNEXT '13, ACM, New York, NY, USA, 2013, pp. 7–12. doi:10.1145/2535372.2535416.
URL http://doi.acm.org/10.1145/2535372.2535416

[35] I. Livadariu, A. Elmokashfi, A. Dhamdhere, On ipv4 transfer markets: Analyzing reported transfers and inferring transfers in the wild, Computer Communications 111 (2017) 105–119.

[36] Internet Society, Google buys a /12 IPv4 Address Block, https://www.internetsociety.org/blog/2017/05/google-buys-a-12-ipv4-address-block/ (2017).

[37] Internet Society, MIT Goes on IPv4 Selling Spree, https://www.internetsociety.org/blog/2017/05/mit-goes-on-ipv4-selling-spree/ (2017).

[38] J. I. Alvarez-Hamelin, L. Dall'Asta, A. Barrat, A. Vespignani, K-core decomposition of Internet graphs: hierarchies, self-similarity and measurement biases, Networks and Heterogeneous Media 3 (2) (2008) 371–293.

[39] S. N. Dorogovtsev, A. V. Goltsev, J. F. F. Mendes, K-core organization of complex networks, Phys. Rev. Lett. 96 (4) (2006) 040601.

[40] C. Orsini, E. Gregori, L. Lenzini, D. Krioukov, Evolution of the internet k-dense structure, IEEE/ACM Trans. Netw. 22 (6) (2014) 1769–1780. doi:10.1109/TNET.2013.2282756.
URL http://dx.doi.org/10.1109/TNET.2013.2282756

[41] M. Faloutsos, P. Faloutsos, C. Faloutsos, On power-law relationships of the internet topology, SIGCOMM Comput. Commun. Rev. 29 (4) (1999) 251–262.

[42] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, k. claffy, As relationships, customer cones, and validation, in: Proceedings of the 2013 Internet Measurement Conference, IMC '13, ACM, New York, NY, USA, 2013, pp. 243–256. doi:10.1145/2504730.2504735.
URL http://doi.acm.org/10.1145/2504730.2504735

[43] R. Pastor-Satorras, A. Vázquez, A. Vespignani, Dynamical and correlation properties of the internet, Phys. Rev. Lett. 87 (25) (2001) 258701.

[44] V. Batagelj, M. Zaveršnik, Fast algorithms for determining (generalized) core groups in social networks, Advances in Data Analysis and Classification 5 (2) (2011) 129–145.

[45] M. G. Beiró, J. I. Alvarez-Hamelin, J. R. Busch, A low complexity visualization tool that helps to perform complex systems analysis, New J. Phys 10 (12) (2008) 125003.

[46] CAIDA, AS Rank, http://as-rank.caida.org/ (07 2018).

[47] T. Böttger, F. Cuadrado, S. Uhlig, Looking for hypergiants in peeringdb, SIGCOMM Comput. Commun. Rev. 48 (3) (2018) 13–19. doi:10.1145/3276799.3276801.
URL http://doi.acm.org/10.1145/3276799.3276801

[48] R. Oliveira, D. Pei, W. Willinger, B. Zhang, L. Zhang, The (in)completeness of the observed internet as-level structure, IEEE/ACM Trans. Netw. 18 (1) (2010) 109–122. doi:10.1109/TNET.2009.2020798.
URL http://dx.doi.org/10.1109/TNET.2009.2020798

[49] Y.-C. Chiu, B. Schlinker, A. B. Radhakrishnan, E. Katz-Bassett, R. Govindan, Are we one hop away from a better internet?, in: Proceedings of the 2015 Internet Measurement Conference, IMC '15, ACM, New York, NY, USA, 2015, pp. 523–529. doi:10.1145/2815675.2815719.
URL http://doi.acm.org/10.1145/2815675.2815719

[50] V. Giotsas, M. Luckie, B. Huffaker, K. Claffy, Ipv6 as relationships, cliques, and congruence, in: J. Mirkovic, Y. Liu (Eds.), Passive and Active Measurement, Springer International Publishing, Cham, 2015, pp. 111–122.

[51] CAIDA, Archipelago (Ark) Measurement Infrastructure, https://www.caida.org/projects/ark/.

[52] Y. Hyun, A. Broido, k. claffy, Traceroute and BGP AS Path Incongruities, Tech. rep., Cooperative Association for Internet Data Analysis (CAIDA) (Mar 2003).

[53] Stefan Meinders, The New Internet, ENOG11 (2016).

[54] CAIDA, Mapping Autonomous Systems to Organizations: CAIDA's Inference Methodology, https://www.caida.org/research/topology/as2org/.

[55] Sandvine, Global internet phenomena report Spring 2011 (2011).

[56] V. Stocker, G. Smaragdakis, W. Lehr, S. Bauer, The growing

complexity of content delivery networks: Challenges and implications for the internet ecosystem, Telecommunications Policy 41 (10) (2017) 1003–1016.
[57] Amazon, AWS global infrastructure, https://aws.amazon.com/es/about-aws/global-infrastructure/ (2017).
[58] Apple Insider, Apple's in-house CDN efforts spell trouble for Akamai as infrastructure biz warns of losses, http://appleinsider.com/articles/16/02/10/apples-in-house-cdn-efforts-spell-trouble-for-akamai-as-infrastructure-biz-warns-of-losses (2016).
[59] ARS Technica, Apple?s multi-terabit, $100M CDN is live - with paid connection to Comcast, https://arstechnica.com/information-technology/2014/07/apples-multi-terabit-100m-cdn-is-live-with-paid-connection-to-comcast/ (2014).
[60] LA Times, Apple's original TV production to begin small: 'We are just starting out', http://beta.latimes.com/business/hollywood/la-fi-ct-apple-television-strategy-planet-apps-20170214-story.html (2017).
[61] Yahoo Finance, Number of active users at Facebook over the years, https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html (2012).
[62] Tom Hormby, The Rise of Google: Beating Yahoo at Its Own Game, http://lowendmac.com/2013/the-rise-of-google-beating-yahoo-at-its-own-game/.
[63] New York Times, Google to Acquire YouTube for $1.65 Billion, http://www.nytimes.com/2006/10/09/business/09cnd-deal.html.
[64] Netflix Media Center, "Announcing the Netflix Open Connect Network", https://media.netflix.com/en/company-blog/announcing-the-netflix-open-connect-network (2012).
[65] Seeking Alpha, Apple, Microsoft And Facebook Bring More Traffic To In-House CDNs, Impacting Akamai's Media Business, https://seekingalpha.com/article/3613736-apple-microsoft-facebook-bring-traffic-house-cdns-impacting-akamais-media-business (2015).
[66] Geoff Huston, Measuring IPv6 Deployment, https://meetings.ripe.net/ripe-56/presentations/Huston-Measuring_IPv6_Deployment.pdf (2008).
[67] Christian Kaufmann, Akamai's V6 Rollout Plan and Experience from a CDN Point of View, MENOG9.
[68] Amazon Web Services, Elastic Load Balancing Announces Support for IPv6, Zone Apex Support and Security Group Integration, https://aws.amazon.com/es/about-aws/whats-new/2011/05/24/elb-ipv6-zoneapex-securitygroups/ (2011).
[69] Amazon, AWS IPv6 Update ? Global Support Spanning 15 Regions & Multiple AWS Services, https://aws.amazon.com/es/blogs/aws/aws-ipv6-update-global-support-spanning-15-regions-multiple-aws-services/ (2017).
[70] Dyn Blog, IPv6: One Operating System at a Time, https://dyn.com/blog/ipv6-one-operating-system-at-a-time-2/ (2015).
[71] Lorenzo Colitti, IPv6 at Google, https://www.ripe.net/participate/meetings/roundtable/february-2009/LorenzoIPv6atGoogle.pdf (2009).
[72] Facebook Engineering, Adding :face: to every IP: Celebrating IPv6's one-year anniversary, https://www.facebook.com/notes/facebook-engineering/adding-face-to-every-ip-celebrating-ipv6s-one-year-anniversary/10151492544578920/ (2009).
[73] Netflix Tech Blog, Enabling Support for IPv6, https://medium.com/netflix-techblog/enabling-support-for-ipv6-48a495d5196f (2012).
[74] Netflix Tech Blog, Building fast.com, https://medium.com/netflix-techblog/building-fast-com-4857fe0f8adb (2016).
[75] Digital Element, NetAcuity, https://www.digitalelement.com/solutions/.
[76] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, B. Gueye, Ip geolocation databases: Unreliable?, SIGCOMM Comput. Commun. Rev. 41 (2) (2011) 53–56. doi:10.1145/1971162.1971171.
URL http://doi.acm.org/10.1145/1971162.1971171
[77] M. Gharaibeh, A. Shah, B. Huffaker, H. Zhang, R. Ensafi, C. Papadopoulos, A look at router geolocation in public and commercial databases, in: Proceedings of the 2017 Internet Measurement Conference, IMC '17, ACM, New York, NY, USA, 2017, pp. 463–469. doi:10.1145/3131365.3131380.
URL http://doi.acm.org/10.1145/3131365.3131380
[78] Quinn, James, Being Open: How Facebook Got It's Edge, NANOG68.
[79] Galperin, Hernan, Connectivity in Latin America and the Caribbean: The role of internet exchange points, Internet Society, November.
[80] CAIDA, CAIDA's AS classification list, http://data.caida.org/datasets/as-classification/.
[81] Twitch blog, Twitch is 4th in Peak US Internet Traffic, https://blog.twitch.tv/twitch-is-4th-in-peak-us-internet-traffic-90b1295af358 (2014).
[82] Business insider, Amazon's streaming service Twitch is pulling in as many viewers as CNN and MSNBC, https://www.businessinsider.com/twitch-is-bigger-than-cnn-msnbc-2018-2 (2018).
[83] J. Deng, G. Tyson, F. Cuadrado, S. Uhlig, Internet scale user-generated live video streaming: The twitch case, in: M. A. Kaafar, S. Uhlig, J. Amann (Eds.), Passive and Active Measurement, Springer International Publishing, Cham, 2017, pp. 60–71.
[84] Peering DB, TWITCH (AS46489) entry at Peering DB, https://www.peeringdb.com/net/1956 (2018).

A first look at the Latin American IXPs

Esteban Carisimo*
Universidad de Buenos Aires
carisimo@cnet.fi.uba.ar

Julián M. Del Fiore
University of Strasbourg/ICube
delfiore@unistra.fr

Diego Dujovne
Universidad Diego Portales
diego.dujovne@mail.udp.cl

Cristel Pelsser
University of Strasbourg/ICube
pelsser@unistra.fr

J. Ignacio Alvarez-Hamelin*
Universidad de Buenos Aires
ihameli@cnet.fi.uba.ar

ABSTRACT

We investigated Internet eXchange Points (IXPs) deployed across Latin America. We discovered that many Latin American states have been actively involved in the development of their IXPs. We further found a correlation between the success of a national IXP and the absence of local monopolistic ASes that concentrate the country's IPv4 address space. In particular, three IXPs have been able to gain local traction: IX.br-SP, CABASE-BUE and PIT Chile-SCL. We further compared these larger IXPs with others outside Latin America. We found that, in developing regions, IXPs have had a similar growth in the last years and are mainly populated by regional ASes. The latter point clearly contrasts with more internationally re-known European IXPs whose members span multiple regions.

CCS CONCEPTS

• **Networks → Public Internet**;

KEYWORDS

Internet eXchange Points, Latin America

1 INTRODUCTION

Latin America covers 20 million km^2 [5] and comprises 20 countries: right after North America, it has the largest urban population rate [6]. Moreover, Latin America (LatAm) is home of 652 million people [52] and has three out of the four largest metropolitan areas in the Americas (Sao Paulo, Mexico City and Buenos Aires with populations of 21.3M, 21.2M and 15.3M habitants respectively) [51]. LatAm also has appealing numbers regarding to Internet: by July 2019, 8661 out of 10171 ASNs delegated to LACNIC currently appear on BGP routing tables. Furthermore, out of 65438 active ASes, 6458 have been delegated by NIC.br (Brazilian NIR) to Brazilian-based organizations. However, few Internet studies have focused on Latin America, let alone their IXPs.

Latin America was on board for the massive irruption of Internet Exchange Points (IXPs) that began in the early 2000s and that contributed to flatten the Internet [17]: it hosts 119 out of 967 IXPs deployed worldwide [29]. Many reasons suggest why IXPs have also widespread in Latin America. First, national IXPs in LatAm are essential to avoid forwarding packets between local end-hosts through thousands-kilometer-long detouring paths [25]. Indeed, the ability to peer locally at IXPs not only shortens paths, but also reduces latency [25]. Second, Latin America has densely populated megalopolis that host a large base of customers of online services and applications. This attracts CDNs that, as an effective way to get to *eyeballs*, use IXPs to peer directly and simultaneously with several ASes [16]. In turn, IXPs are also interested in hosting CDNs, to provide cost-effective access to content to their members [22].

Compared to regions such as North America and Europe, *Latin America is short of resources for Internet measurements*. For instance, Routeviews [53] (RVs) and RIPE RIS [47] only have two and one BGP data collectors in LatAm, respectively. The lack of collectors only allows to draw a fairly incomplete representation of the AS ecosystem in Latin America [35]. On the other hand, little active-measurement-derived analysis can be performed in LatAm (e.g. to unveil paths from/to content providers) due to a limited availability of active vantage points (as of July 2019, RIPE Atlas (311/10,209), Ark CAIDA (12/190)).

In this paper, we take a closer look at the Latin American IXPs. We are interested in the public policies that lead to their creation, their growth and development over time, and the role they play in their own national AS ecosystem. In particular, in Sec. 2, we introduce the dataset we built to carry out our analysis:

- We identify multiple BGP collectors of Packet Clearing House (PCH) that provide valuable data of the Latin American AS ecosystem. Moreover, we manually extended the BGP view in Brazil leveraging several Looking Glasses (LGs) that are available and distributed in the network of the Brazilian IXP.
- We use AS relationship, RIR delegation, and prefix mapping files to derive metrics that help quantify the growth of IXPs and to better understand the role of transit providers at IXPs.

Our contributions are:

- We provide insights in Sec. 3 about how countries' public policies have encouraged the development of IXPs in Latin America.
- We propose several metrics in Sec. 4 and 5 that allow to account how IXPs have been increasingly gaining importance since their creation and how this phenomena correlates with the presence of a balanced AS ecosystem, i.e., the absence of monopolistic transit/access ASes.
- We compare IXPs deployed across multiple continents and find that IXPs in developing regions share similar properties.
- We release the code that allows both to fetch the publicly available data we used and to replicate our results[1]. In addition, we make publicly available the LGs' dumps we manually collected[2].

*Also with CONICET - Universidad de Buenos Aires. Instituto de Tecnologías y Ciencias de la Ingeniería "Hilario Fernández Long" (INTECIN). Buenos Aires, Argentina.

[1]Project repository: https://github.com/CoNexDat/latam-ixp-obs
[2]LG dumps: https://cnet.fi.uba.ar/latam-ixp-obs/lg-ribs/

2 DATASET

Our dataset relies primarily on BGP table dumps (BGP-TDs) obtained from collectors deployed across multiple LatAm countries. We also manually gathered BGP-TDs in LGs available in Brazil. In addition, we used RIR delegation, CAIDA's AS relationship and *pfix2as* files, PeeringDB and other digitalized documents. Next, we detail these sources.

BGP-TDs: we use BGP-TDs from the collector of RVs in Sao Paulo, Brazil (BR)[3]. The first snapshots dumped in this collector date from 2011. We also rely on PCH's "IPv4 Daily Snapshot" archive to obtain a long-standing collection of feeds, even dating from 2010 in some cases, from Argentina (AR), Belize (BZ), Chile (CL), Costa Rica (CR), Ecuador (EC), Haiti (HT), Honduras (HN), Mexico (MX), Paraguay (PY) and Trinidad and Tobago (TT)[4]. Indeed, with 15 monitors co-located at IXPs in multiple countries of LatAm, PCH is, by July 2019, the route collecting project with the largest footprint in the region.

In addition, to put our results in context, we also downloaded BGP-TDs from PCH collectors in other regions: France-IX (Paris), DE-CIX (Frankfurt, Germany), JINX (Johannesburg, South Africa) and BKNIX (Bangkok, Thailand). We chose these IXPs because either themselves, or the countries where they are deployed, share properties with those deployed in LatAm: largest populations in their region (e.g. France, Germany and Brazil), similar age (e.g. BKNIX and the Chilean IXP are recently created IXPs, while DE-CIX and the Argentinian IXP have been both operating for more than two decades) and comparable current values of GDP per capita (e.g. South-east Asia, South Africa and Latin America) [7].

All BGP-TDs of RVs and PCH were collected the first day of each month. We observed that some ASes share full tables, and we believe that this not what actually gets advertised in the IXPs, i.e., following Gao-Rexford principles [36], no AS would offer cost-free transit via its upstream providers. Consequently, when analyzing each IXP, we relied only on entries provided by their route server: in these cases, the revealed routes are usually from ASes advertising their customers, at least partially. Finally, all BGP-TDs were sanitized removing AS-path prepending and dropping entries with AS sets (less than 1%). While BGP-TDs may not able be to capture the entire AS topology, overcoming this incompletenesses requires traceroute-derived data [27], a limited resource in LatAm (see the introduction).

Finally, we enlarged the BGP data collected in Brazil using the LGs publicly accessible via telnet in IX.br [9], the network interconnecting the Brazilian IXPs. Unfortunately, IX.br does not keep historical LGs' BGP-TDs. By running "`show ip bgp paths`", we gathered BGP-TDs in the 31 regional IXPs of IX.br in July 2019. Despite only partial-BGP-TDs can be obtained in Sao Paulo and Curitiba [9], this does not affect our analysis, as explained in Sec. 4.2.

RIR delegation files[5]: we queried LACNIC delegation files to determine the set of ASes delegated to each country. However, it must be noted that nationality in RIR delegation files does not actually indicate that an AS only or mainly operates in the country to which the ASN was delegated to, but it does show that the organization that holds the ASN has economical activities in that country. Further, our goal is not to precisely determine ASes location, but rather from where the companies that join the IXPs come from.

CAIDA's AS relationship and prefix2AS files[6]: while the former were used to pinpoint *active* ASes each month, i.e., with at least one inferred AS relationship, the latter were used to compute the address space originated by each AS.

PeeringDB [42]: we used PeeringDB to retrieve IXP's Route Server ASNs and to validate inferences.

Digitalized Documents: we gathered digitalized documents concerning Internet's public policies applied by LatAm's governments, e.g. legal documents, newspapers, websites, presentations.

3 PUBLIC POLICIES AND IXPS

We investigated the public policies behind the creation of IXPs in Latin America. For this, we relied on the set of digitalized documents we gathered. Table 1 shows the organizations that currently run these IXPs and that fostered their creation. All in all, **out of 16 national IXPs currently operating in LatAm, governments were involved in the creation of more than 55% of them.**

The president of Costa Rica signed an Executive Order [45, 48] while parliament in Bolivia passed a law [25]. Also, federal agencies such as Senatics in Paraguay [28], PUC in Belize [50] and SENACYT in Panama [30] fostered IXP's creation. Regulators were involved in Mexico (IFT) [39], Honduras (CONATEL-HN) [15] and Paraguay (CONATEL-PY) [31]. In Brazil, the Internet Steering Committee (CGI), a multi-stakeholder board with several state representatives, was responsible for creating IX.br, the Brazilian IXP [3]. On the other hand, Table 1 also indicates that, similar to the European IXP model [10], in Latin America a large number of non-profit organizations created and run IXPs. In particular, CABASE (AR) and CCIT (CO) are operated by organizations related to local ISPs associations as it happens in IXPs outside the region, e.g. DE-CIX (DE) [13] and JINX (ZA) [33]. Further, Belize, Honduras and Paraguay have delegated IXP operations to universities. Finally, presence of state regulations also influenced the development of peering facilities in Chile. Undersecretary of telecommunications singed Resolution 1483 [49] in 1999 which forced traffic between Chilean ISPs to be carried by their local infrastructure. To fulfill this requirement, ISPs rapidly joined NAP Chile, a Chilean IXP. More recently, in 2016, PIT Chile was established on top of the dense interconnected infrastructure of NAP Chile, though bringing significant changes to the Chilean peering ecosystem: whereas NAP Chile was strictly limited to domestic ASes, PIT Chile was envisioned as a neutral IXP also allowing the presence of non-national ASes.

4 EVOLUTION OF IXPS

Many of the IXPs in Latin America have already been running for years. Consequently, we aim to understand whether these IXPs have been able to consolidate in their region, as so have others in different geographical areas. We look at IXPs': i) network topology ii) members, i.e., connected networks; iii) ASes connected via members (visible ASes), and; iv) transit providers role. Most countries that host a BGP monitor (see Table 1) have small IXPs (e.g. with less than 30 connected networks that announce less than 2M unique

[3] http://routeviews.org/route-views.saopaulo
[4] PCH has presence in a Bolivian IXP with no members [38], that is thus not considered.
[5] ftp://ftp.lacnic.net/pub/stats/lacnic/
[6] data.caida.org/datasets

Country	AR	BO	BR	BZ	CL	CO	CR	CU	EC	HT	HN	MX	PA	PY	PE	TT
Sponsored by	CABASE	Law	CGI	PUC	PIT CL	CCIT	Ex.Ord.	State	IXP.EC	AHTIC	CONATEL	IFT	SENACYT	SENATICS	NAP.PE	TTIX
Operated by	CABASE	State	NIC.br	UoBZ	PIT CL	CCIT	NIC.cr	NAP.CU	IXP.EC	AHTIC	UNAH	CITI	InteRED	NIC.py	NAP.PE	TTIX
BGP TDs	Monitor	PCH	×	RVs/LGs	PCH	PCH	×	PCH	×	PCH	PCH	PCH	PCH	×	PCH	×	PCH
	#Memb	127		1156	6	72		28		5	4	4	6		15		5
	#AggIPs	7.9M		26M	67K	19.4M		401K		28K	102K	131K	795K		1.5M		196K

Table 1: IXPs in Latin America. Colors blue, yellow and magenta represent state agencies, non-profit organizations and universities, respectively. #AggIPs is computed on the address space announced by IXP members (excluding their customer cone and repeated prefixes due to MOASes). LatAm countries without IXPs and European overseas territories are excluded.

IPs). Since this limits the conclusions that can be drawn in them, our analysis mainly focuses on the bigger IXPs of AR, BR and CL.

4.1 IXP Networks Topology

We used PeeringDB, digitalized documents and previous knowledge, to look for organizations that run multiple IXPs in LatAm. We found that, as of July 2019, IX.br, CABASE and PIT Chile run 31, 28 and 6 regional IXPs respectively in Brazil, Argentina and Chile. Next, we would like to study how these organizations coordinate and interconnect their IXPs. In CABASE, regional IXPs such as CABASE-BUE (AS11058) or CABASE-COR (AS52374), are independent and have their own ASNs. In addition, they are all connected to a central node, CABASE-RCN (AS52376), that just interconnects the IXPs (it is not a regional IXP that has members). Through CABASE-RCN, a *Mandatory Multilateral Peering Policy* (MMPP) is enforced: prefixes advertised in one regional IXP are further advertised by the central node in all regional IXPs, as can be seen in Fig. 1 for CABASE-BUE and CABASE-COR. We further verified this contrasting PCH's BGP-TDs collected in multiple of regional IXPs of CABASE. On the other hand, PIT Chile is structured as CABASE: regional IXPs are also connected to a central node, PIT Chile-SCL (AS61522), but that is actually a regional IXP itself. While Chilean regional IXPs are visible as members of PIT Chile-SCL, since PIT Chile only hosts a collector in the latter regional IXP and does not impose any peering policy, we cannot ensure if the reciprocate is also valid. Finally, IX.br runs a single ASN (AS26162) and does not have a centralized topology.

4.2 IXP Members

To identify IXP members or *connected networks* of every regional IXP we used BGP-TDs dumped in July 2019. In particular, for CABASE-BUE and PIT Chile-SCL we got them from PCH, and for IX.br from its LGs. Note that the need of data from an unique collector in CABASE and PIT Chile, but from many for IX.br, results from the fact the first two have a central node in their network (see Sec. 4.1). While in CABASE we used tables from CABASE-BUE, which is not the central node but sees all announcements due to the MMPP imposed, for PIT Chile we got them from PIT Chile-SCL, their central node. On the other hand, since IX.br does not have a central node, we used a LG per regional IXP. Finally, IXP members were inferred as the first AS found in each AS path after the IXP's ASNs (e.g., Route Server, regional IXPs). We further verified that, despite the LGs' BGP-TDs in Sao Paulo (SP) and Curitiba (PR) are partial (see Sec. 2), the number of members seem not to be compromised: while RV sees 1156 peers in IX.br-SP, the LG in the same regional IXP reports 1164.

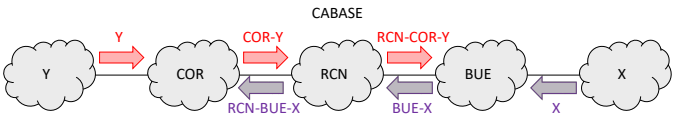


Figure 1: Topology of CABASE (for 2 regional IXPs) and its Mandatory Multilateral Peering Policy. Arrows indicate BGP announcements and their respective AS path. RCN is a central node that interconnects regional IXPs (e.g. BUE, COR) and forwards all announcements to all regional IXPs.

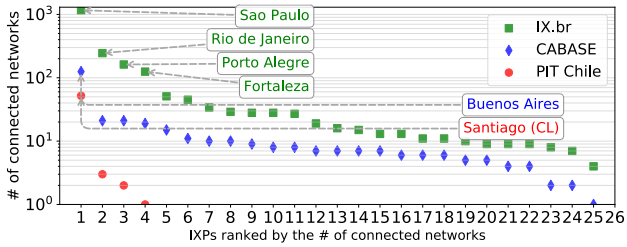


Figure 2: Number of connected networks to regional IXPs in IX.br, CABASE and PIT Chile in July 2019.

Fig. 2 displays the number of connected networks per regional IXP in IX.br, CABASE and PIT Chile (in the ones missing of IX.br and PIT Chile, BGP-TDs showed no members). In the three IXPs, the largest regional IXP is around an order of magnitude bigger than the second one: -Sao Paulo: 1156, Rio de Janeiro: 245- in BR, -Buenos Aires: 127, Cordoba: 21- in AR and -Santiago de Chile: 72, Arica: 3- in CL. The population of the metropolitan areas where the regional IXPs are deployed seems to have an impact on this result, with 21.3, 6.3, 15.3, 1.8 and 5.6 million inhabitants respectively in Sao Paulo, Rio de Janeiro, Buenos Aires, Cordoba and Santiago de Chile. Considering that these Latin American IXPs mainly attract local ASes (see Sec. 4.3), the number of delegated-and-active ASes in each country, with 6458, 791 and 241 respectively in BR, AR and CL, might also explain the difference in size between them.

4.3 Visible ASes

ASes connected via members, or *visible ASes*, correspond to the set of ASes seen in BGP-TDs, i.e. that appear in the AS paths of prefixes announced at the IXP. This metric is relevant since, despite some ASes might not be members of the IXP, they might still indirectly benefit from it. We are interested in the impact of IXPs in their domestic region, and also in how many foreign networks are attracted to Latin American IXPs. Moreover, we want to understand if IXPs in other regions show similar behaviors. To perform this analysis, we used PCH's BGP-TDs for all IXPs, except for IX.br where we

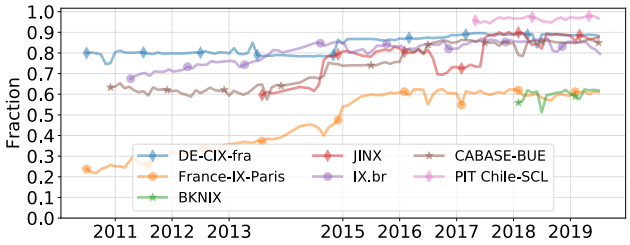


Figure 3: Fraction country's delegated-and-active ASNs visible at the IXPs.

used data from RVs. In addition, we used RIR delegation files to determine the set of ASNs delegated to each country.

4.3.1 Domestic impact. First, leveraging CAIDA's AS relationship files, we determined *all* delegated-and-active ASNs for each country, and thus for each IXP. For this, we simply filtered out delegated but inactive ASNs, i.e., ASNs with no inferred AS relationships. Then we looked for ASes that: i) are visible in each IXP and; ii) are local, i.e., own an ASN delegated to the country where the IXP is deployed. Fig. 3 displays the ratio of local visible ASes to *all* delegated-and-active ASNs for the biggest IXPs in Latin American: IX.br-SP, CABASE-BUE and PIT CL-SCL. Moreover, the figure also shows results for France-IX, DE-CIX, JINX and BKNIX.

Fig. 3 reveals that 80% of the Brazilian and Argentinian country delegated-and-active ASNs are visible at IX.br-SP and CABASE-BUE, respectively. This fraction is similar to the one observed in DE-CIX (Frankfurt) and by far larger than in France-IX (Paris), despite the large wealth gap (i.e. GDP per capita) between the European Union and Latin America [7]. Indeed, even though LatAm spans a larger geographical extension, IXPs of the region have still managed to deploy an infrastructure that allows them to host a large fraction of their local ASes. In addition, while DE-CIX has been stuck in this fraction value since 2011, CABASE-BUE and IX.br-SP have been steadily growing since the beginning of the decade when they just had around 60%. The Brazilian IXP network growth in the past decade was driven by the investments in telecommunications to host the 2014 FIFA World Cup as well as the 2016 Summer Olympics [18, 34]. On the other hand, CABASE's fraction of visible ASes, as well as number of regional IXPs, has increased since Google joined the IXP in late 2011.

In addition, Fig. 3 also shows that PIT Chile-SCL, that started operating in 2016, has a striking fraction of 90% even from the first snapshot we got from the PCH collector in 2017. This is the highest historical value in Latin America, and indeed high for an infant IXP: for example, BKNIX, which was launched in 2015, covers just 60% of the current delegated-and-active ASNs in Thailand. To grow rapidly, PIT Chile leveraged Chilean public policies (see Sec. 3).

Finally, note that JINX, the IXP in South Africa, has also been increasing the fraction of visible country delegated-and-active ASNs over time. The similarities with the IXPs in Brazil and Argentina in terms of the same 20% of increase and the fact that the three IXPs have reached a value comparable to a big IXP such as DE-CIX, allows to speculate on a matureness process that replicates across continents: regions where the Internet is rather underrepresented seem to, after many years, have been able to attract as many local ASes as some well-established IXPs in Europe.

4.3.2 Foreign networks attraction. Fig. 4 shows[7] the prevalence of AS nationalities at each IXP, i.e., out of all visible ASes in an IXP, how many come from each country. As can be seen, the three bigger Latin American IXPs mainly provide local support: the largest fraction of visible ASes, around 75% in all cases, are from the countries where the IXPs are deployed. However, these IXPs are also able to extend to other countries in the region, which usually add up most of the remaining fraction in Fig. 4. These results are similar to the ones seen in BKNIK and JINX. Indeed, all these IXPs are not so internationally widespread, i.e., the ASes they host come from less than 50 different countries in all cases. All this is in clear contrast with what happens in European IXPs that rather act as international hubs: not only the number of visible nationalities is greater than 100 for France-IX and over 200 for DE-CIX, but also most of their visible ASes are actually not local regarding to where the IXPs are deployed (France-IX not shown). Despite these differences, it is remarkable that the US is always within the five most prevalent AS nationalities[8] for all IXPs: this is likely due to the advertisement of prefixes of relevant US-based companies (e.g., Google, Facebook, Netflix, CloudFlare, Fastly). Indeed, the fact that CDNs find in IXPs a way to remain close to their customers and to offer them a better service is particularly also true in Latin America, Asia and Africa.

4.4 Transit Providers

We are interested in how traffic is carried from/to Latin American IXPs by transit providers, i.e., intermediary ASes between IXPs and origin ASes seen in those IXPs. More precisely, since ASes in LatAm could be potentially scattered throughout vast geographic extensions, we would like to identify transit providers that have contributed to the consolidation of IXPs in their local country. Therefore, we look at the size of the set of visible ASes *per upstream AS*, i.e. the set of unique ASes that appear after each AS in AS paths. For this we used BGP-TDs dumped in July 2019 by PCH and RVs.

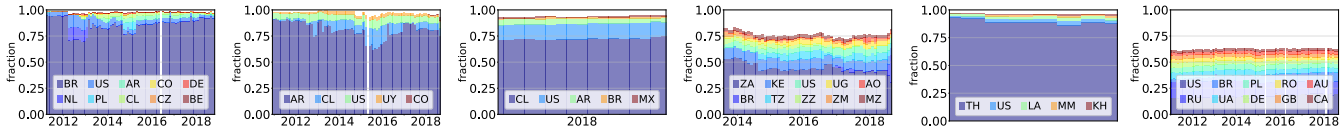
Table 2 displays for IX.br-SP, CABASE-BUE and PIT Chile-SCL the five upstream ASes that announced the largest visible AS sets. Results show a richer AS ecosystem in Brazil: Algar (AS16375) alone announces more downstream ASes in IX.br-SP than all the visible ASes seen in CABASE-BUE as well as in PIT Chile-SCL. On the other hand, looking at the nationality of the TOP5 upstream ASes in each IXP, we see mainly domestic transit providers. Yet, there are exceptions: Internexa (AS262589, Colombia (CO)) and Silica (AS7049, AR) in IX.br, Level3 (AS3549, US) in CABASE-BUE and Internexa (AS52880, CO) in PIT Chile-SCL.

In addition, Table 2 shows that Level3 is the largest upstream AS in CABASE-BUE (AS3549) and, though not displayed in Table 2, also ranked sixth in PIT Chile-SCL (AS21838, legacy number of an acquired network [40]). We further investigated Level3's role in both IXPs and determined that this US' ISP actually acts as a domestic transit provider in LatAm: 204 out of 209 and 37 out of 43 downstream ASes announced by Level3 in CABASE-BUE and PIT Chile-SCL were delegated by LACNIC to AR and CL, respectively.

Finally, Table 2 also unveils the presence of state-owned ISPs among the largest upstream ASes: Internexa (AS262589, AS262195)

[7] For this analysis, we filtered out the large number of prefixes announced by Hurricane Electric (AS6939), probably just on account of its open peering policy [26], in IX.br, JINX, DE-CIX and France-IX.

[8] By nationality we mean an AS that have been delegated to the US



(a) IX.br-SP (b) CABASE-BUE (c) PIT Chile-SCL (d) JINX (e) BKNIX (f) DE-CIX-fra

Figure 4: Prevalent AS nationalities at IXPs in Latin America, Africa, Asia and Europe.

IX.br-SP	ASN	16735	262589	7049	61832	28329
	#	903	381	218	209	207
CABASE-BUE	ASN	3549	52361	7049	19037	11664
	#	219	113	100	82	81
PIT Chile-SCL	ASN	7004	22661	52280	19228	14259
	#	88	87	70	57	57

Table 2: Largest sizes (#) of visible AS sets *per upstream AS* in IX.br-SP, CABASE-BUE and PIT Chile-SCL.

and ARSAT (AS52361). Internexa is a partially state-owned Colombian AS in which the Ministry of Finance and Public Credit holds 51% of the shares while Medellin county (Colombia) holds another 10% [1]. On the other hand, ARSAT (AS52361) is a fully state-owned Argentinian transit provider [37]. Note that, while ARSAT's transit service focuses in Argentina, Internexa's transit footprint comprises foreign countries, such as Argentina and Brazil.

5 IXPS AND CONCENTRATION

We believe that the presence of monopolistic ASes may discourage the deployment/growth of IXPs. Hence, we look if the IPv4 address space delegated to Latin American countries is fairly distributed, i.e., if no AS owns most IP prefixes assigned to a country.

For this analysis, we queried CAIDA's *pfix2as* files of July 2019 and LACNIC delegation files. While the first were used to determine the set of *active* prefixes (seen in routing tables) and the ASes that originate them, the latter allowed to check the countries to which these network blocks had been delegated to. In the end, the combination of both datasets outputs a database indicating, for each Latin American country, all active prefixes and the ASes that originate them. However, we acknowledge some limitations of this methodology. First, prefixes delegated by other RIRs (not LACNIC) might be active in LatAm. Second, we cannot determine which of the announced addresses are actually used [12]. Third, prefixes delegated by LACNIC to Latin-American-based ASes can be used beyond the region. Fourth, presence of Carrier Grade NAT (CGN) could cause underrepresentation of ASes that, though originate small address space, have a large number of subscriptions, especially for mobile carriers [46]. While the use of geolocation databases may mitigate these problems, these sources are known to be inaccurate in many cases [43]. Consequently, refining the methodology followed to detect active prefixes in each country is left as future work.

We leveraged our database to compute the Herfindahl-Hirschman Index (HHI), a statistical measure of concentration that ranges from 1 (single monopolistic origin) to 0. This metric is used by the US Department of Justice to apply antitrust regulations [44] and in ecology to measure diversity (known as *Simpson's Diversity Index*). Fig. 5 displays HHI for Latin American countries with more than 1M delegated IP addresses. The right end shows countries with low concentration ratio, such as Brazil, Chile and Argentina. Indeed, these countries host the largest IXP networks. On the contrary, the left side includes countries such as Uruguay, Dominican Republic

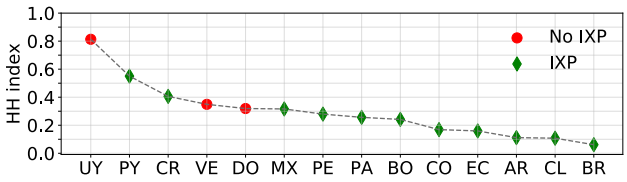


Figure 5: Herfindahl-Hirschman Index to determine originated address space concentration in countries that have been delegated more than 1M IP addresses.

	UY		VE		CR		MX	
ASN	6057*	19422	8048*	6306	11830*	52228	8151	13999
ip-cnt$_{cc}$	2.38M		5.15M		2.42M		24.9M	
ip-cnt	2.15M	90.1k	2.84M	629k	1.52M	197k	13.7M	2.05M
ip-frac	0.90	0.04	0.55	0.14	0.63	0.08	0.55	0.08

Table 3: The two largest origin ASes per country. ∗ indicates state-owned ASes.

and Venezuela, that do not have any IXP, and Paraguay, Costa Rica and Mexico, all possessing an HHI of more than 0.3.

We take Uruguay, Venezuela, Costa Rica and Mexico as cases of study and display in Table 3 the first and second dominant ASes that concentrate most of the IPs delegated to these countries. In all cases, the first dominant AS not only originates between 55% to 90% of its respective national address space, but also owns at least 47% more than the second. In particular, countries dominated by large state-owed providers such as Venezuela (CANTV) and Uruguay (ANTEL) are not even planning to release an IXP [14, 24]. Costa Rica is the opposite example: while the state owns ICE, the main ISP that originates 63% of the national address space, the first national IXP was created by an executive order in 2014 (see Sec. 3). Remarkably, ICE has never joined the IXP [41]. Mexico is another country with high HHI whose IXP just has 6 members. We suspect that, despite the fact that the creation of the IXP in 2014 was sponsored by the Mexican government as a recommendation of the OECD [11], the absence of Telmex (AS8151) [32], by far the first dominant AS in the country, discouraged the IXP growth.

6 RELATED WORK

Although Latin America is underrepresented in Internet measurement projects, some studies have specifically looked at this region. Berenguer *et al.* [8] studied how the BGP view of RIPE RIS and RouteViews in LatAm can be extended by additionally using BGP dumps collected in looking glasses of the region. Brito *et al.* [9] carefully studied the composition and interconnection of Brazilian public exchange network in three snapshots, and then compared Brazilian IXP size in terms of connected networks and peering policy prevalence with IXPs in other regions. Formoso *et al.* [23] used RIPE Atlas probes in Latin America to create an inter-country latency matrix as a way to detect fairly asymmetric paths and poorly interconnected countries.

In addition, there is a vast body of literature that studied IXPs. Dhamdhere *et al.* studied how IXPs contributed to the AS ecosystem and to flatten the Internet [17], while Augustin *et al.* carefully quantify the number of peering links seen at IXPs [4]. Other papers also analyzed the anatomy of a large European IXP [2] as well as the role of IXPs in the African AS ecosystem [19–21].

7 CONCLUSIONS AND FUTURE WORK

This study contributes four findings regarding to Internet topology research. First, we found that Latin American states have been involved in the creation of national IXPs in several ways: legislation, regulation, sponsoring, funding, operations and serving traffic from/to IXPs. Second, we discovered three consolidated IXPs, IX.br-SP, CABASE-BUE and PIT Chile-SCL, that gather mainly local but also regional ASes. Third, we compared these IXPs with others deployed in other continents and found that some IXPs in developing regions not only have had a similar growth in the last years, but also seem to have reached matureness, i.e., have been able to attract as many local ASes as so do some well-established IXPs in Europe. However, European IXPs have also managed to gather members from different regions, a market that could be exploited in the future by the less renown, and rather local, IXPs in Latin America, Asia and Africa. Fourth, we studied the correlation between the existence of ASes concentrating address space, and the IXP development and consolidation. Indeed, in several Latin American countries the existence of monopolistic ASes, some state-owned, seem to have prevented the proliferation of IXPs.

This work suggests several promising directions. First, our work could be extended by studying CDN deployment in LatAm and their co-location at IXPs. Second, we would like to compare IXP peering policies throughout LatAm IXPs. Third, we want to investigate IPv6 rollout in LatAm and the role of IXPs in such process.

ACKNOWLEDGMENTS

Authors would like to thank anonymous operators in Latin American IXPs as well as members of ISOC-LAC for validating our inferences. This work was partially funded by UBACyT 2018 (grant number: 20020170100421BA). This work has been published under the framework of the IdEX Unistra and benefited from a funding from the state managed by the French National Research Agency as part of the "Investments for the future" program.

REFERENCES

[1] Accionistas ISA. 2019. http://www.isa.co/es/nuestra-compania/Paginas/quienes-somos/composicion-accionaria.aspx. (2019).
[2] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger. 2012. Anatomy of a large European IXP. *CCR* 42, 4 (2012), 163–174.
[3] E. Ascenco. 2015. Peering in Brazil. https://ix.br/doc/nic.br.ptt.br.ais-sandiego.20150405-02.pdf. (2015).
[4] Brice Augustin, Balachander Krishnamurthy, and Walter Willinger. 2009. IXPs: mapped?. In *IMC 2009*. 336–349.
[5] World Bank. 2016. World Development Indicators: Rural environment and land use. http://wdi.worldbank.org/table/3.1. (2016).
[6] World Bank. 2018. The World Bank data: Urban population. https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS?page=1. (2018).
[7] World Bank. 2019. GDP per capita in LAC, EU, East Asia, TH, ZA. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=ZJ-EU-Z4-TH-ZA&year_high_desc=false. (2019).
[8] S. S. Berenguer, E. Carisimo, J.I. Alvarez-Hamelin, and F. V. Pintor. 2016. Hidden internet topologies info: Truth or myth?. In *LANCOMM 2016*. 4–6.
[9] S. H. B. Brito et al. 2016. Dissecting the Largest National Ecosystem of Public Internet eXchange Points in Brazil. In *PAM 2016*.
[10] Nikolaos Chatzis, Georgios Smaragdakis, Anja Feldmann, and Walter Willinger. 2013. There is more to IXPs than meets the eye. *CCR* 43, 5 (2013), 19–28.
[11] CITI. 2014. Inauguración del Primer IXP Mexicano. http://www.ixp.mx/noticias/14_04_30_inaguracion.php. (2014).
[12] Alberto Dainotti et al. 2016. Lost in space: improving inference of IPv4 address space utilization. *IEEE J. Sel. Areas Commun.* 34, 6 (2016), 1862–1876.
[13] DE-CIX. 2019. History of DECIX. https://bit.ly/2tuVHW2. (2019).
[14] Camara de Telecomunicaciones de Uruguay. 2019. El monopolio de Antel. http://www.telecomunicaciones.org.uy/index.php/el-monopolio-de-antel/. (2019).
[15] DEGT. 2016. Lanzan IXP-HN. https://blogs.unah.edu.hn/degt/lanzamiento-del-punto-de-intercambio-de-trafico-de-internet-de-honduras-ixp-hn/. (2016).
[16] Amogh Dhamdhere and Constantine Dovrolis. 2008. Ten years in the evolution of the internet ecosystem. In *IMC 2008*. 183–196.
[17] Amogh Dhamdhere and Constantine Dovrolis. 2010. The Internet is flat: modeling the transition from a transit hierarchy to a peering mesh. In *CoNEXT 2010*. 21.
[18] Governo do Brasil. 2014. R$ 1.8 Billion in Telecommunications Investments for 2014 FIFA World Cup. https://bit.ly/2OA86jp. (2014).
[19] Roderick Fanou et al. 2018. A System for Profiling the IXPs in a Region and Monitoring their Growth: Spotlight at the Internet Frontier. *IJNM* (2018).
[20] Rodérick Fanou, Pierre Francois, and Emile Aben. 2015. On the diversity of interdomain routing in africa. In *PAM 2015*. 41–54.
[21] Rodérick Fanou, Francisco Valera, and Amogh Dhamdhere. 2017. Investigating the Causes of Congestion on the African IXP substrate. In *IMC 2017*. 57–63.
[22] Peyman Faratin. 2007. Economics of overlay networks: An industrial organization perspective on network economics. In *Proceedings of the NetEcon+ IBC workshop*.
[23] Agustin Formoso and Pedro Casas. 2016. Looking for network latency clusters in the lac region. In *LANCOMM 2016*. 10–12.
[24] Freedom House. 2018. Freedom on the Net 2018: Venezuela. https://freedomhouse.org/report/freedom-net/2018/venezuela. (2018).
[25] Hernán Galperín. 2016. Localizing Internet infrastructure: Cooperative peering in Latin America. *Telematics and Informatics* 33, 2 (2016), 631–640.
[26] Vasileios Giotsas, Matthew Luckie, Bradley Huffaker, and Kc Claffy. 2015. IPv6 AS relationships, cliques, and congruence. In *PAM 2015*. 111–122.
[27] Hamed Haddadi et al. 2010. Mixing biases: Structural changes in the AS topology evolution. In *TMA workshop*. Springer, 32–45.
[28] Ultima Hora. 2015. Proyecto de Senatics ayudara a abaratar acceso a internet. https://www.ultimahora.com/c864692. (2015).
[29] Packet Clearing House. 2019. Internet Exchange Directory. https://www.pch.net/ixp/dir#\protect\kern-.1667em\relaxmt-sort=reg%2Cdesc. (2019).
[30] InteRED. 2019. InteRED. http://intered.org.pa/intered/. (2019).
[31] ITU. 2016. Consultoria - IXP Paraguay. https://bit.ly/2Lay76N. (2016).
[32] ITU. 2016. IXP Mexico. https://bit.ly/2R5PCZL. (2016).
[33] JINX. 2019. About INX-ZA. https://www.inx.net.za. (2019).
[34] Julimar L. 2008. Resultados Copa do Mundo. ftp://ftp.registro.br/pub/gter/gter41/02-IX.br-update.pdf. (2008).
[35] Anukool Lakhina, John W Byers, Mark Crovella, and Peng Xie. 2003. Sampling biases in IP topology measurements. In *IEEE INFOCOM 2003*, Vol. 1. 332–341.
[36] Lixin Gao and J. Rexford. 2001. Stable Internet routing without global coordination. *IEEE/ACM Transactions on Networking* 9, 6 (2001), 681–692.
[37] Mapa del Estado. Jefatura de Gabinete de Ministros de Argentina. 2019. https://mapadelestado.jefatura.gob.ar/organismos.php. (2019).
[38] Mario Durán Chuquimia. 2013. Seminario sobre el PIT. http://desarrollotics.blogspot.com/2013/07/preparando-un-seminario-tecnico-sobre.html. (2013).
[39] IFT México. 2016. Consulta Publica. https://bit.ly/2OxPdxB. (2016).
[40] La Nacion. 2006. GBLX adquirió Impsat. https://www.lanacion.com.ar/economia/global-crossing-adquirio-impsat-por-us-336-millones-nid853038. (2006).
[41] La Nacion. 2015. ICE rechaza unirse a sistema para agilizar Internet a usuarios. https://bit.ly/37DSS3v. (2015).
[42] PeeringDB. 2016. https://www.peeringdb.com. (2016).
[43] Ingmar Poese, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP geolocation databases: Unreliable? *CCR* 41, 2 (2011), 53–56.
[44] S. A. Rhoades. 1993. The Herfindahl-Hirschman Index. (1993).
[45] MICITT (Costa Rica). 2019. IXP Costa Rica: Una oportunidad estrategica. https://micit.go.cr/index.php?option=com_content&view=article&id=6329. (2019).
[46] Philipp Richter et al. 2016. A multi-perspective analysis of carrier-grade NAT deployment. In *IMC 2016*. 215–229.
[47] RIPE NCC. 2019. RIPE Routing Information Service (RIS). https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris. (2019).
[48] SCIJ. 2014. Decreto Ejecutivo 38388. https://bit.ly/2FljQ41. (2014).
[49] SubTel. 1999. Resolucion 1483. https://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/res_1483conexiones_entre_isp.pdf. (1999).
[50] TeleGeography. 2016. Belize gets internet exchange point; BIXP becomes twelfth such facility in Caribbean. https://bit.ly/2sxgisc. (2016).
[51] UN. 2016. The World's Cities in 2016. https://bit.ly/36uMpaW. (2016).
[52] UN. 2017. World Population Prospects 2017. https://population.un.org/wpp/Download/Standard/Population/. (2017).
[53] University of Oregon. 2019. RouteViews. http://www.routeviews.org/. (2019).

Identifying ASes of State-Owned Internet Operators

Esteban Carisimo*
Northwestern University

Alexander Gamero-Garrido
CAIDA, UC San Diego
Northeastern University

Alex C. Snoeren
UC San Diego

Alberto Dainotti
CAIDA, UC San Diego
Georgia Institute of Technology

ABSTRACT

In this paper we present and apply a methodology to accurately identify state-owned Internet operators worldwide and their Autonomous System Numbers (ASNs). Obtaining an accurate dataset of ASNs of state-owned Internet operators enables studies where state ownership is an important dimension, including research related to Internet censorship and surveillance, cyber-warfare and international relations, ICT development and digital divide, critical infrastructure protection, and public policy. Our approach is based on a multi-stage, in-depth manual analysis of datasets that are highly diverse in nature. We find that each of these datasets contributes in different ways to the classification process and we identify limitations and shortcomings of these data sources. We obtain the first data set of this type, make it available to the research community together with the several lessons we learned in the process, and perform a preliminary analysis based on our data. We find that 53% (*i.e.,* 123) of the world's countries are majority owners of Internet operators, highlighting that this is a widespread phenomenon. We also find and document the existence of subsidiaries of state-owned governments operating in foreign countries, an aspect that touches every continent and particularly affects Africa. We hope that this work and the associated data set will inspire and enable a broad set of Internet measurement studies and interdisciplinary research.

ACM Reference Format:
Esteban Carisimo, Alexander Gamero-Garrido, Alex C. Snoeren, and Alberto Dainotti. 2021. Identifying ASes of State-Owned Internet Operators. In *ACM Internet Measurement Conference (IMC '21), November 2–4, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3487552.3487822

*The author partially worked on this article during his time at Universidad de Buenos Aires and CONICET.

IMC '21, November 2–4, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-9129-0/21/11…$15.00
https://doi.org/10.1145/3487552.3487822

1 INTRODUCTION

In this paper, we introduce and apply a methodology to accurately identify state-owned Internet operators worldwide and their Autonomous System Numbers (ASNs). Obtaining an accurate dataset of state-owned Internet operators' ASNs enables research studies where state ownership is an important dimension, including many Internet phenomena that have salient socio-economic or political implications: Internet censorship and surveillance, cyber-warfare and international relations, Information and Communications Technology (ICT) development and the digital divide, critical infrastructure protection, and public policy. Autonomous system numbers represent a key variable to bridge these dimensions with the technical domain: not only they are central to studies involving the Internet topology, but they have an (almost) *one-to-one* mapping with IP addresses[1], which thus inherit some of their ASNs' properties and vice versa.

Despite such importance, a data set providing this information was not available before our study. Few commercial business information databases provide ownership information for companies worldwide but *(i)* they do not carry any data related to ASes and *(ii)* in this study we find that they might not be entirely accurate and comprehensive (in the context of Internet operators). Previous Internet measurement literature discussed the role of selected ASes operated by state-owned providers in one or two specific countries or regions in *e.g.,* specific Internet censorship events [24, 62] or in the development of a country's peering infrastructure [19]. Other research efforts focused on AS taxonomization and classification either from a topological perspective [26, 28] or in terms of business type (but focused on an individual country for which public databases already exist) [82]. Hard challenges include indeed the scarcity of data on a global scale and the fact that this is a multidisciplinary problem.

We tackle this research problem by proposing a multi-stage method based on datasets that are highly diverse in nature and an in-depth manual analysis that takes into account complex ownership structures. We also reduce the problem complexity by narrowing our focus to operators *(i)* of significant size, *(ii)* operating at national (*e.g.,* federal) level, and *(iii)* who do not restrict their services to only certain sectors (*e.g.,* exclusively research and education).

We obtain the first—to the best of our knowledge—data set of this type, we make it available to the research community together with the several lessons we have learned in the process, and we perform a preliminary analysis based on our data. Reinforcing the

[1] Almost all routed IP addresses are originated in the global routing system by only one AS.

relevance of this subject, we find that *state-ownership is a broad global phenomenon* but much more prevalent in Africa and Asia (blue and green countries in the heatmap in Figure 1—discussed in detail in § 8). We also find and document the existence of subsidiaries of state-owned companies operating in foreign countries (green countries in Figure 1), an aspect that touches every continent and particularly affects Africa.

Our key contributions are the following:

(1) A novel methodology to identify state-owned ASes of Internet operators worldwide, which we verify through manual analysis and cross-comparison of multiple data sources.
(2) The first publicly available data set containing the full list of state-owned ASes of Internet operators, including metadata referencing each organization to the corresponding input and confirmation sources.
(3) Being this a novel research challenge we gained significant insights, for example regarding the quality and characteristics of the data sources as well as the intricacies of the problem. We document and discuss them in detail.
(4) We find 989 state-owned ASes—including 193 ASes of state-owned providers operating abroad—of 123 countries. Combining this data set with other Internet data, we find preliminary results suggesting that the prevalence of state-owned providers in the Internet access market is substantially higher in Asia and Africa. We also find that African countries host a remarkable presence of foreign state-owned ASes and in 6 of these countries foreign state-owned ASes hold more than 50% of the estimated access market.

We hope that this work and the associated data set will inspire and enable a broad set of Internet research studies.

2 CHALLENGES

Identifying state-owned telecommunication companies and the ASes they operate is a multifaceted problem crossing various technical and administrative domains. In this section we summarize the most critical challenges, which are largely based on limitations of the available data.

Lack of public databases: There is no global public registry that indexes state-owned enterprises. Only a few countries (*e.g.,* Sweden [52], Finland [53] and Uruguay [25]) report, through public websites, which companies have state participation. Moreover, specificity and granularity of the data vary from country to country. Focusing on the topic of our study, telecommunication companies, we are unaware of any publicly available resource that lists, at a global- or regional-level, all telecommunication companies, nor one that only specifies state-owned telcos. For instance, the United Nations ITU [76] is (at least partially) aware of state participation in telecommunication companies. In fact, some ITU reports do mention the presence of state-owned telcos. However, there is no central repository or simple way to identify and access the ITU documents that include this specific information. Moreover, isolated reports are not sufficient to create a world's list of state-owned telcos.

We have identified two commercial databases that provide information about ownership of telecom enterprises: Orbis [80] and Telegeography's GlobalComms [72]. However, their methodologies and the frequency of updates are not disclosed in detail and it is unclear how accurate they are. We include Orbis data in our study and find it misses or misclassifies a few companies in terms of state-ownership. Despite following the directions on the Telegeography website in an attempt to evaluate or purchase their product, we did not receive a response and were therefore unable to evaluate this dataset.

Company-to-AS mapping: Relying on accurate company names is necessary to determine state participation. However, there is a lack of databases and methodologies that allow us to precisely map ASes to companies and vice versa. WHOIS databases from Regional Internet Registries (RIR) [55] map ASNs to the names of the companies that they were delegated to. However, WHOIS records may not be updated as an AS or company ownership/denomination changes, leading to inaccurate and obsolete information [83] (despite ICANN initiatives to enhance WHOIS such as the WHOIS Accuracy Program Specification [47]). Moreover, a company's registration name (`OrgName` field), which tends to be the company's legal name, may differ from commercial names or brand names. As an example, Colombia's state-owned *Internexa* operates AS262195 in Argentina, however LACNIC's WHOIS records report the owner's name as *Transamerican Telecomunication S.A.*

In addition, telecom companies sometimes own more than one ASN (for historical or technical reasons and because of acquisitions/mergers); these are called *sibling* ASNs. Sibling ASNs can be associated with very different names in WHOIS, making state-of-the-art WHOIS-based sibling inference methods [17, 18] unable to capture the entire of set of ASes operated by the same organization.

Complex and evolving ownership structures: Detecting state participation in a company requires checking for state presence across shareholders and through indirect chains of ownership (*i.e.,* control over a company's shareholders through state-controlled companies). The aggregated participation of multiple state-controlled bodies—such as hedge, wealth and pension funds—at companies' shareholder structures could give control to the state. For example, three of Malaysia's government-owned funds—Khazanah Nasional Berhad [10], Amanah Raya Berhad [9] and the Employees' Pension fund [5, 6, 29]—in aggregate hold more than 50% of the shares of Telekom Malaysia (AS4788) [11].

Large state-owned telecom companies also operate subsidiaries and branches abroad. E.g., Qatar's state-owned Ooredoo operates several subsidiaries across North Africa and the Middle East (Algeria, Tunisia, Kuwait, Oman *etc.*). Companies do not use homogeneous ways to report subsidiaries and branches—or vice versa if they are controlled by a parent organization—making it challenging to correctly identify relationships between parent and child companies. In addition, for legal purposes, companies sometimes register subsidiaries abroad to be able to run business activities in other countries, without necessarily associating a new ASN with them. This potential behavior adds another layer of uncertainty to *company-to-AS mapping*, since when no ASN is found for a given network operator company, it is unclear whether the mapping failed or the company actually does not own an ASN. For example, China Telecom operates subsidiaries in Brazil and Canada [70] but we believe these companies do not operate their own ASN.

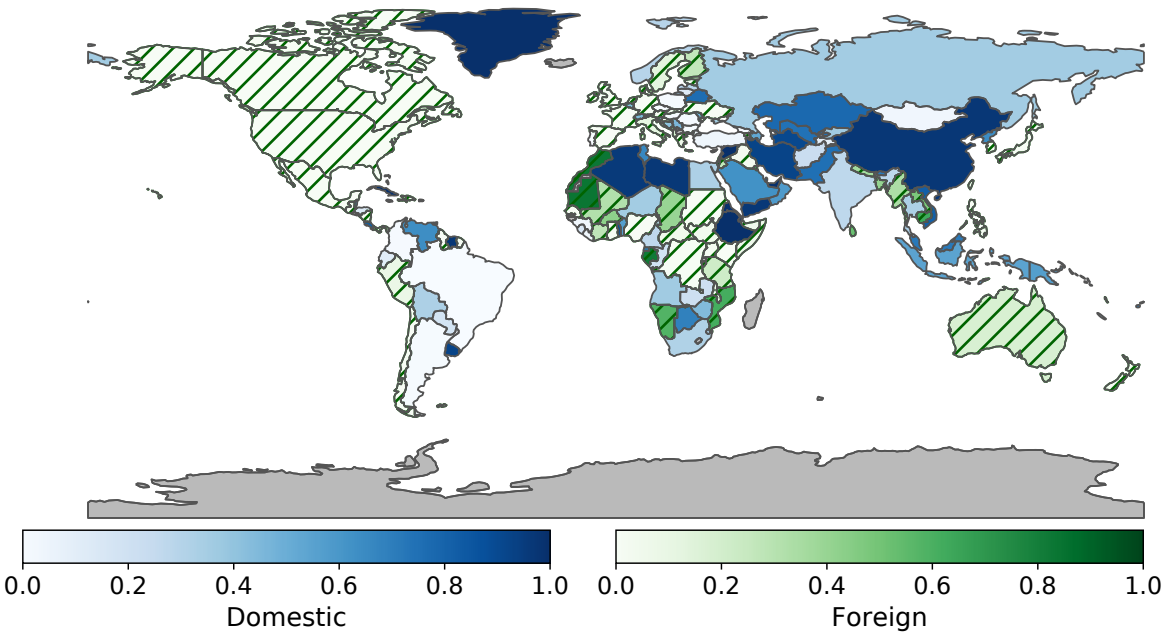


Figure 1: Footprint of state-owned Internet operators. In blue: The maximum between *(i)* the fraction of address space geolocated in the country that is originated through BGP by ASes owned by the same country and *(ii)* the fraction of eyeballs (according to APNIC Eyeballs dataset) from ASes owned by the same country. In green (lines): The same calculation but considering ASes owned by other countries.

Finally, ownership of telecommunication companies is very dynamic, and tracking these changes is challenging for three reasons. First, governments communicate privatizations and (re-)nationalizations in fairly diverse ways, including public releases, public acts, media conferences, or communications at stock exchanges. Second, variations of the state ownership of telecommunication companies happen frequently. E.g., Ucell, a subsidiary of Swedish minority-state-owned Telia's with presence in Uzbekistan, was acquired by Uzbekistan's government in 2018 [42, 78]. An example in the opposite direction is that while Angola's government has announced several times over the past 4 years its intention to privatize Angola Telecom [4, 22, 43] this transition has not yet occurred. Third, due to the size of the international telecommunication market, it is impractical to continuously monitor the shareholder structure of all telcos to detect changes on state participation.

3 METHODOLOGY OVERVIEW

Definition of state-owned AS. There is no commonly accepted definition of state-owned enterprise. The IMF, the OECD and the European Commission use different criteria [35]. However, these institutions agree on three elements to define a firm as state-owned: *(i)* the company has its own separate legal entity, *(ii)* the entity is partially controlled by a government unit, and *(iii)* the entity engages in commercial or economic activities. In this paper, we use these same criteria and, regarding point *(ii)*, we follow the IMF definition stated in the IMF's Fiscal Monitor report released in April 2020, Chapter *State-Owned Enterprises: The Other Government* [35], which considers a firm as state-owned if the government owns at least 50% of its equity[2]. In our study we specifically focus on federal-level (or equivalent) companies offering transit or unrestricted access to Internet connectivity (*i.e.*, we do not include in our definition companies operating only at subnational level). We call these companies *Internet operators* and—in the context of this paper—we define *state-owned AS* an AS owned by a state-owned Internet operator (*i.e.*, a state-owned Internet operator is in control of the AS number delegated by a Regional Internet Registry).

Data Discovery and Classification. Our process has three stages, which are depicted in the diagram in Figure 2. At a high level: we identify ASNs and company names (stage 1) to obtain a candidate list of companies to be manually verified (stage 2). During manual verification we also filter and enrich this data. An example of filtering is the exclusion of operators with minority state participation, whereas enrichment includes adding subsidiary companies. We conclude the process by obtaining a final list of ASNs operated by the selected companies and generating our final dataset (stage 3).

Reference Timeframe. We emphasize that the data we obtain as part of this process captures the state ownership of ASes during a specific time frame. For this research we generated the candidate lists and analyzed company ownership structures from June 2019 to November 2020. As mentioned in § 2, ownership structures are dynamic, and while we mitigate this risk, state ownership of these

[2]While we note that some literature suggests that a government may exercise significant influence over corporate decisions even when it owns a small number of shares [34], we cannot quantify government-exerted influence in these circumstances.

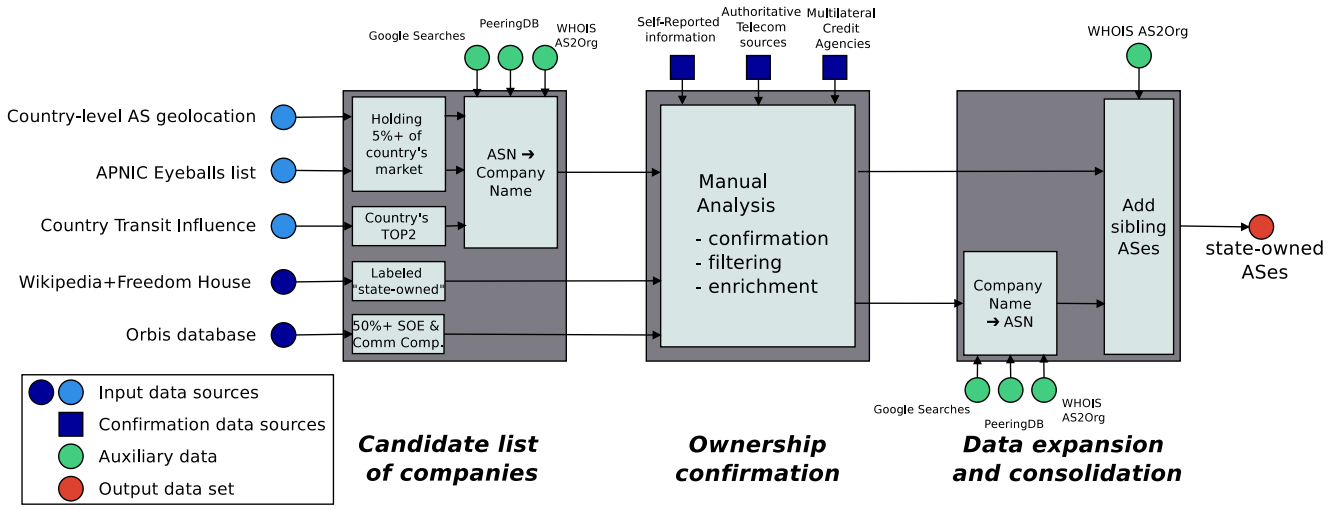


Figure 2: Block diagram of our data discovery and classification process. We describe it from left to right. Stage #1: We use five input sources (technical in light blue and non-technical in dark blue) to obtain a candidate list of potentially state-owned companies. Stage #2: For each company, we manually verify whether a federal-level government owns its majority. In addition, in this stage we filter operators with minority state participation. We also add subsidiary companies to the list of state-owned ASes. Stage #3: We add sibling ASNs obtaining a final list of ASNs operated by the selected companies. We then generate our final dataset.

companies might have changed even within the duration of this study. In § 9 we discuss the subject of dataset ageing.

4 CANDIDATE ASES AND COMPANIES

We bootstrap our process by analyzing multiple and varied data sources, represented as blue circles on the left-hand side of Figure 2, through which we select data to be manually examined in the next stage of our methodology (§ 5). These candidate data can be of two distinct types: *(i)* ASNs whose ownership we intend to verify or *(ii)* company names that according to our sources are (likely) state-owned and thus require us to verify such information. We call (Computer Networking) *Technical Sources* (§ 4.1) those from which we obtain lists of ASes, which we then map to actual company names (§ 4.2). We refer as *Non-technical Sources* (§ 4.3) to data sources from which we instead obtain names of companies reported as state-owned.

4.1 Candidate ASes

Technical Sources allow us to identify ASes providing Internet services and infer their country-specific market relevance. We use three different sources and approaches, which we describe in the following paragraphs: Country-level AS geolocation, APNIC eyeballs dataset, key transit providers in each country.

Country-level AS geolocation: We geolocate globally-routed network prefixes to identify the geographical footprint of every AS originating IP address space. We use CAIDA's prefix-to-AS list from July 1st, 2019 to obtain all pairs of BGP-routed prefixes and their correspondent origin ASes for the 68,283 visible ASes in the global routing table. We then use Digital Element's *NetAcuity Edge* IP geolocation service [27] to determine the (country-level) location of every IP address of each routed prefix.[3] The IP-level granularity of the geolocation process allows us to create a list of triplets containing *<Origin ASN (OASN), country, number of IP addresses that OASN originates in that country>*.

We limit the candidate list of providers to later examine for possible state ownership to networks with significant market share. We thus exclude ASes that originate less than 5% of a country's globally-routed IP addresses, obtaining a total of 793 ASes (≈1% of the total number in this dataset). This threshold should be sufficient to include all state-owned ASes that operate major access networks in each country.

APNIC eyeballs dataset: We rely on the number of "eyeballs" reported by APNIC to determine the most populated networks in each country. While estimating the population of Internet users of an AS is challenging due to the widespread use of NAT [66], APNIC has developed heuristics to estimate the eyeball populations leveraging web-based advertising [46]. APNIC's estimations report the eyeball population for 25,498 ASes. We use their estimates of AS eyeballs population as an additional variable to measure the market size of access networks. Similarly to what we do for the Country-level AS geolocation approach, we select only ASNs with an estimate of at least 5% eyeballs in a given country. We obtain a list of 716 unique ASes (≈3% of the total number in this dataset), which interestingly is a comparable—but smaller—number of ASes to those obtained through Country-level AS geolocation. There are 466 ASes in the intersection of both data sources and we obtain 1043 ASNs from the union of both.

[3] While geolocation databases are known to be unreliable at fine granularities, previous work has found them to be more accurate at the country level [14, 60], with Netacuity in particular having accuracy between 74–98% [39].

Countries' main upstream providers: Finally, we shift our attention from large *access* networks to key *transit* connectivity providers. Specifically, we use the Country-Level Transit Influence (CTI) metric [38] to select key transit networks providing international access in several countries. CTI is a BGP-based metric that captures the fraction of a country's IP addresses that are served by a particular transit network (AS). Formally, the transit influence of autonomous system *AS* on country *C* is the weighted fraction of *C*'s address space for which *AS* is present on announced, preferred paths toward prefixes originated in *C* by a responsive AS that is visible in public BGP data [1, 2]. We include a more precise formulation in Appendix G.

In countries where transit providers (as opposed to peers) have been inferred as the dominant inbound modality [38], CTI allows us to identify a country's reliance on specific transit providers granting international connectivity. We hypothesize that in such countries the government may be engaged in deploying domestic transit connectivity. In fact, states have created diverse alternatives, such as establishing transit gateways connecting domestic ASes with international transit providers (*e.g.,* Syria's AS29386-Syrian Telecom), building national backbones (*e.g.,* Argentina's ARSAT-AS52361), or in some cases building their own submarine cable networks (*e.g.,* Angola's AS37468-ACS, Bangaldesh's AS132602-BSCCL or the WIOCC consortium—AS37662—in which some state-owned African ISPs hold shares).

CTI [3] has been applied in 75 countries comprising 1,314 unique ASes. In each of these countries we select the two highest CTI-ranked ASes for inclusion in our candidate list of ASes, resulting in 93 ASes (≈7% of the total number in this dataset).

4.2 Mapping ASes to their companies

When we combine the three technical sources we obtain a total number of 1091 ASes, which in total belong to 1023 different organizations, according to CAIDA's AS2Org data. We use WHOIS records and entries from PeeringDB [57] to identify the companies owning these ASes. We start from WHOIS records, since this is compulsory information required by RIRs from each organization requesting an AS number. Although WHOIS records have a per-RIR data structure, a few fields are common across all RIRs, such as ASN, AS name, organization, and at least one email and/or phone contact.

To mitigate errors in WHOIS records, we also use PeeringDB, a website providing a non-compulsory database of self-reported data. PeeringDB covers roughly 20% of the ASes registered in the WHOIS. Operators register their ASNs on PeeringDB to share information about peering or operational tasks (*e.g.,* how to contact NOC 24x7x365 teams in case of a failure) and to be visible on the platform in order to *e.g.,* attract more (transit) customers and peers. It is therefore in the interest of these ASes to keep their information up to date and we assume that the company names there reported are similar or identical to the brand names in order to facilitate their identification.

When unable to find any website mentioning the company names we obtained from WHOIS and PeeringDB, we Google-search for the DNS domains from the point of contacts there were listed, *e.g.,* URLs or emails. In these searches we found that the challenge in mapping these companies tends to be related to name alterations after rebrands, mergers and acquisitions. In general, AS-to-company mapping is challenging and requires further study.

4.3 Candidate Companies

We extend our data with names of telecom companies identified as state-controlled by our selected Non-Technical Sources.

Orbis: We query the commercial Orbis database to obtain a list of state-owned telecommunication companies. Orbis is produced by Bureau van Dijk's, a Moody's Analytics company that collects and distributes datasets with company information to financial risk assessors and governments [51, 81]. Orbis is a business information database containing information on more than 400 million companies and entities around the world, including their corporate ownership structures [80]. Orbis has been used in scientific publications in business and economic research fields [8, 13, 44, 50, 63] as well as in reports by national and international organizations, including the NBER [48], the OECD [37] and the World Bank [56]. Related to our work, a previous research study used Orbis to identify state-owned telecommunication companies in Africa [33] but to analyze the relationship between Internet shutdowns and the state ownership of Internet providers. Using the Orbis database engine filters we find telecommunications companies in which sovereign states own more than 50% of the equity, resulting in 994 companies.

Freedom House report & Wikipedia articles: We also add to our list companies reported as state-owned in Freedom House reports and in Wikipedia articles. Freedom House's Freedom of the Net project releases annual reports on each country's "Internet freedom". Freedom of the Net measures interventions by governments and non-state actors aimed at restricting Internet rights, and covers 65 countries. The reports are produced by in-country activists, civil society groups, academics, journalists, and tech and legal experts.

We also use Wikipedia to expand the candidate list of *candidate* state-owned companies. We find that two types of Wikipedia articles tend to include information about state-owned telcos: articles describing the country's communication landscape and articles listing the country's state-owned enterprises. We repeat this searching process for every country. We do not take state ownership in these articles at face value: we validate this information in the second stage of our process which will remove false positives (Figure 2). However, we expect Wikipedia articles and Freedom House reports to contain false negatives (*i.e.,* these reports and articles might miss some state-owned telcos): we mitigate such false negatives by including data from all the other data sources here discussed.

5 OWNERSHIP CONFIRMATION

In the second stage (Figure 2) of our process we manually examine the companies from the candidate state-owned list. We verify their ownership structure and business sector, we extend our examination to subsidiaries and parent companies, and we filter out organizations that do not strictly match our definition of state-owned Internet operator.

5.1 Confirmation data sources

To investigate the ownership structure of companies from our candidate list, we rely on manually consulting the following authoritative sources.

Self-reported information. We primarily look at company websites, government websites and corporate annual reports. In some countries (*e.g.,* Norway), transparency legislation requires their governments to fully disclose state participation in companies. When states hold shares of publicly-traded corporations, corporate ownership structures (and therefore state participation) are publicly available in the corporate annual reports. In other cases, websites of state-owned telcos explicitly declare the state control of the company, such as in Congo's CONGTEL website [69].

Authoritative telecommunication sources. We also rely on authoritative telecommunication sources such as the US SEC, the FCC, local regulators and the ITU. These regulators and organizations have purview over commercial and technical aspects of telecommunication companies, and their freely available documents may refer to the ownership structure of the company. Companies with commercial activities in the US (it may be the case of foreign state-owned companies) are subject to submit filings to US regulators such as the SEC and the FCC. Similarly, local regulators may request and disclose details of domestic companies, including state ownership. With a different set of goals, the ITU operates at international level and runs multiple commissions to promote infrastructure development and to assist developing countries [79]. These commissions regularly release documents and meeting materials which sometimes includes information about a country's telecom landscape. We use articles released by *CommsUpdate*, a well-known source of telecom news stories worldwide [20]. Its publisher, Telegeography, is a telecom market research company [20]. Several CommsUpdate articles include information about state-owned companies in their research on Internet markets.

Credit agencies. We use reports published by research and financial departments of multilateral credit agencies, such as the World Bank and the International Monetary Fund (IMF), describing countries telecom markets and including the presence of state-owned incumbents. Most of these reports are publicly available through the World Bank library, *e.g.,* [4].

5.2 Discovering state-owned subsidiaries

When manually investigating the ownership structure of the companies from our candidate list, we also look for parent state-controlled companies to identify subsidiaries. This way we actually discover *additional* companies that are not detected by our list of candidate companies.

Interestingly, we find that some state-owned subsidiaries provide Internet services in foreign countries. We define (and label in our output dataset) as *foreign state-owned subsidiary* a separate legal entity meeting two conditions: *(i)* whose state-owned parent's (or parents') holdings encompass more than 50% of the shares and *(ii)* that is registered in a foreign country. By capturing such features we hope to enable studies that cross socio-political domains: While governmental involvement in domestic Internet markets is often related to the mandate of economic prosperity, digital inclusion, and national cyber-defense, those factors do not apply when they operate abroad. A country's interest in extending operations abroad might instead be the intent of expanding into other profitable markets, or be a consequence of the nation's goals on international relations.

5.3 Excluded state-funded organizations

Following our definition in § 3, we exclude companies and ASes operated by all subnational jurisdictions: first-level (states, provinces, ...), second-level (municipalities, districts, ...), third-level (cities) or smaller administrative divisions. We remove companies belonging to lower than country-level administrative divisions to reduce the size of our problem and to avoid potential bias. To get a sense of the size, the ISO 3166-2 standard defines more than 5000 identifying codes for first-level administrative divisions (as of March 2021). Furthermore, it is unlikely that our data sources have uniform coverage across countries when considering a fine administrative granularity, which would have caused our dataset to be biased.

Based on our definition (§ 3), we also exclude state-run organizations offering access or transit services restricted to only certain sectors—*e.g.,* academic networks. While some of the excluded networks are owned by government organizations aimed at granting Internet access to certain restricted populations, *e.g.,* to close the digital divide or to connect educational institutions, they do not fall within our scope: federally-funded companies offering services to people and companies as any other commercial ISP would do. However, in Appendix E, we provide some insight about the excluded categories of companies.

6 DATA EXPANSION & CONSOLIDATION

In the last stage of our process (Figure 2), we map confirmed state-owned Internet operators to AS numbers, using—in reverse—the same methodology we apply in § 4.2. We then expand the list of confirmed state-owned ASes by including their sibling ASes using CAIDA's AS2org data [17, 18]. In conducting our analysis (§§ 4, 5), we also identified several sibling ASNs that were incorrectly not recognized as such by AS2Org (*e.g.,* because their AS names are completely different); we contributed our findings to the AS2Org project.

As the result of this process, we obtain two data products: a list of state-owned organizations and a mapping between these organizations and the ASNs they own. We save this data into an SQLite database (which we also export in JSON format) which is publicly available[4]. Listing 1 provides an example from our dataset, showing data for the Norwegian network operator Telenor in JSON format. In the list of state-owned organizations we include four types of fields:

- *Information specific to the organization*: name of the conglomerate the company belongs to, the CAIDA's AS2Org Org ID, the name of the organization, ISO-3361 country code, country name, country's RIR.
- *Confirmation sources that validated the inference*: type of confirmation source (*e.g.,* Company's website), the quote we use to determine the state ownership, the language of the quote, the URL to the confirmation data source and, in some cases, additional information (*e.g.,* specifying that a hedge

[4]The dataset is available here: https://github.com/estcarisimo/state-owned-ases

fund is state-owned). One added benefit of these fields is that they facilitate verifying in the future if the classification is still valid.

- Which *input sources* caused this organization to be originally added to the candidate list. We abbreviate the inputs sources using the following convention: G=Country-level AS geolocation; E=APNIC eyeballs dataset; C=Country Transit Influence; O=Orbis; W=Wikipedia & Freedom House.
- If the company is a *foreign subsidiary*: the parent company's Org ID, the name ('target_country_name') and ISO-3361 country code ('target_cc') of the country where it operates; in this case the 'ownership_cc' and 'ownership_country_name' fields refer instead to the country of the parent company.

```
# Ownership details of an identified
# state-owned organization
{
  "conglomerate_name": "Telenor",
  "org_id": "ORG-NA38-RIPE",
  "org_name": "Telenor Norge AS",
  "ownership_cc": "NO",
  "ownership_country_name": "Norway",
  "rir": "RIPE",
  "source": "Company's website",
  "quote": "Major Shareholdings: Government
    of Norway (54,7%)",
  "quote_lang": "English",
  "url":"https://www.telenor.com/investors/
    share-information/major-shareholdings"
  "additional_info": "",
  "inputs": [G, E, W, O],
  "parent_org":,
  "target_cc":,
  "target_country_name":,
}
# List of ASes operated by the identified
# state-owned organization
{
  "org_id": "ORG-NA38-RIPE",
  "asn": [2119, 8210, 8394, 8786, 39197,
    197943, 200168]
}
```

Listing 1: Example from our dataset for the Norwegian network operator Telenor (AS2119).

7 TAKEAWAYS FROM THE PROCESS

Applying our semi-manual classification process we extract insight about this previously unexplored problem and make several findings which we summarize in this section.

At the end of our process we obtain 989 state-owned ASes—including 193 foreign subsidiaries—from a total of 302 state-owned companies. In aggregate, state-owned ASes originate 17% of the Internet's address space announced in BGP. This fraction increases to 25% if we exclude the US, which does not have state-owned providers and is overrepresented in the global address space due to several largely unused but announcedaddress blocks [23]. Each data source contributes a comparable number of state-owned ASes (between 500 and 640, we include details in Appendix B), except for CTI (12 ASes)—which is expected, since it selects a very specific and narrow class of ASes.

***All* sources provide a unique contribution.** Interestingly, we find[5] that *each* data source contributes a unique set of ASes that no other data source captures. The unique contribution (9 ASes of 12) from the CTI dataset is perhaps the most surprising: most of them are companies exclusively providing transit, *i.e.,* not directly serving a large user population; likely because of the nature of their business, they fly under the radar of the other sources even if they are critical for Internet communications (we provide details about these companies in the Appendix D). These findings confirm our intuition that a broad and diverse set of data sources is needed in order to comprehensively identify state-owned ASes and that existing commercial databases (like Orbis) alone are not sufficient to tackle this problem.

To provide more details on this phenomenon, in Figure 3 we show the Venn diagram of the contributions when grouping the sources in 3 categories based on their diverse nature: *(i)* popular/relevant ASes (Technical Data Sources), *(ii)* sources focused specifically on state-ownership (Wikipedia and Freedom House), and *(iii)* a commercial business information database (Orbis). While 193 ASes are

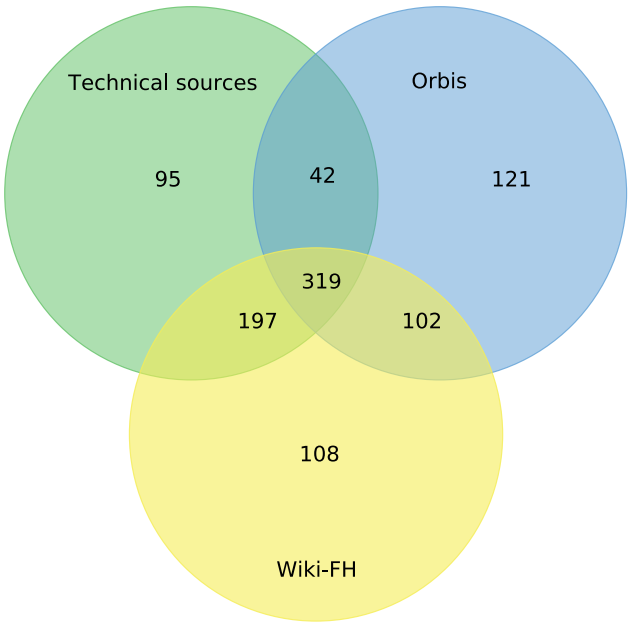


Figure 3: Venn diagram showing overlap and individual contributions of each class of data sources.

shared among all three categories, each category provides significant unique input. In particular, it is interesting that the Technical

[5]Full Venn's diagram in the Appendix C.

Confirmation source	Companies
Company's website	161
Company's annual report	44
Freedom House	33
TG's commsupdate	22
World Bank	20
ITU	6
FCC	4
News	2
regulator	2
Others	9

Table 1: Contribution of each type of confirmation data sources.

Data Sources yield a quite significant number (95) of ASNs that were not found through the others.

Company websites are the major source of confirmation. We then examine which *"confirmation sources"* allowed our manual analysis to verify the state-ownership of the 302 companies — including 84 foreign subsidiary companies— that own these 989 ASes (Table 1). The companies' websites are the most prevalent source of data, covering roughly 50% of the companies.

Freedom house is a reliable source. Freedom House is the second confirmation source: When a company is labeled as state-owned by Freedom House's *Freedom of the Net* report, in most cases we are able to manually confirm through other sources. However, for 42 companies we could not find any authoritative, external sources confirming or refuting Freedom House's assessment. Also, we did not find any false positives of Freedom House's state-ownership assessment. We believe that Freedom House is a reliable source, since it relies on countries' experts to generate their reports, and it is thus safe it to also use it at this stage of our process.

Other authoritative but non-comprehensive sources. Finally, data from reports of the world's largest multilateral credit agencies, the World Bank, and the IMF allowed us to confirm 25 companies (Table 1). However, based on our experience we believe that due to their role, these institutions are more likely to report information for the countries they provide aid to, which are mostly in the developing world.

Insights about using a commercial database. Through the confirmation process we found Orbis incorrectly labels as state-owned 12 companies (false positives) and misses to include, or does not label as state-owned, 140 companies (false negatives). Most of the false positives are foreign subsidiaries. 3 of 12 are wrongly assigned to the Colombian government: 2 are labelled as federally-owned while in fact they are owned by counties, the third one—*Comunicación Celular de Colombia* (formerly *COMCEL*, now *Claro*)—is owned by the private conglomerate América Móvil [65, 71].

Orbis' false negatives are spread across 79 countries. Most of these companies are small and/or in the developing world (Latin America, Central Asia, Southeast Asia and Africa). In the LACNIC region Orbis does not capture *any* state-owned telcos in 11 of the 14 countries in which we find state-owned telcos. For example, Argentina's ARSAT and Uruguay's ANTEL are in the Orbis database but are not labelled as state-owned. We note similar limitations in Central Asia, where Orbis reports no state-owned telcos in Iran, Kazakhstan, Uzbekistan and Tajikistan, and only partially covers Azerbaijan (*e.g.,* in Azerbaijan, Orbis did not report BakTelecom, which Freedom House correctly reports as state-owned). We also observed lack of coverage in Vietnam where for example Freedom House reports state-owned providers.

Third-party validation. We further validated our resulting dataset as much as possible with the help of local experts. We obtained feedback from two local experts. The first one has knowledge of the entire LACNIC region, being a scientist specialized in ICT development who also worked at a regional operator consortium with presence across the entire LACNIC region. The second local expert is an engineer from France specialized in computer networks and working at AFNIC [32]. The expert in Latin America validated the 35 ASNs we identified in the region (belonging to 14 countries) while the one in France validated our findings for the two French companies we have found. In both cases, the experts reported neither false positives or false negatives in our data.

Large ASes with government minority ownership. In our manual analysis, we also identified 302 minority state-owned ASes, which we excluded from our generated dataset based on our definition (§ 3): we did not specifically search for minority participation but we took note of the cases that we encountered in our process, which clearly represent a subset of all ASes with state-minority participation. Among them, we find some large players such as Deutsche Telekom (AS3320, Germany's equity: 31%) [73], Orange (AS5511, France's equity: 22.95%) [54], Telia (AS1299, Sweden's equity: 39.5%) [74] and Bharti Airtel (AS9498, Singapore's SingTel equity: 35.1%) [67, 68].

Multi-government joint ventures. Interestingly, we find instances where two governments jointly own a firm. This is the case of PTCL (AS17557) and Telkomsel (AS23693) are companies owned by two countries, Pakistan and the UAE [41, 61], and Indonesia and Singapore [75], respectively. However, in both firms one country holds the largest equity in the company, Pakistan in PTCL (70%) and Indonesia in Telkomsel (65%). This was also the case of BICS (AS6774), a long-term joint business between Belgium and Switzerland that ended in February 2021 when Belgium's Proximus acquired the rest of the shares of the company [12].

8 A FIRST LOOK AT STATE-OWNED ASES

In this section, we combine our list of state-owned ASes with other data to study the footprint of state-owned ASes in the world.

A global view. Table 2 summarizes the state ownership of Internet operators at a country-level granularity. We find that 53% (*i.e.,* 123) of the world's countries are majority owners of Internet operators, highlighting that this is a widespread phenomenon. We also find that state-owned companies of 19 countries control subsidiaries offering Internet services abroad. The table also shows that at least 24 countries have minority ownership of Internet operators (§ 7). Note that some countries may appear in multiple categories; for example, Singapore owns the majority of the equity of SingTel (AS7473), which operates Optus in Australia (AS7474) and is also a minority owner of Telkomsel (AS23693) in Indonesia.

Table 4 shows the state ownership of telcos at a RIR-level granularity. In all RIRs except ARIN, more than 40% of the country

Participation in	# of countries
state-owned operators	123
subsidiaries	19
minority state-owned operators	24
Total countries	136

Table 2: Number of countries we detected to own Internet operator businesses.

Owner country (cc)	#	Country Codes of the subsidiaries
UAE (AE)	12	AF, BF, BJ, CI, EG, GA, MA, ML, MR, NE, TD, TG
China (CN)	9	AU, GB, HK, MO, NL, PK, SG, US, ZA
Qatar (QA)	9	DZ, ID, IQ, KW, MM, MV, OM, PS, TN
Norway (NO)	9	BD, DK, FI, MM, MY, PK, SE, TH, UK
Vietnam (VN)	9	BI, CM, HT, KH, LA, MZ, PE, TL, TZ
Singapore (SG)	6	AU, HK, JP, KR, LK, TW
Malaysia (MY)	5	BD, ID, KH, LK, NP
Colombia (CO)	4	AR, BR, CL, PE
Serbia (RS)	3	AT, BA, ME
Indonesia (ID)	3	MY, SG, TL
Bahrein (BH)	3	IM, JO, MV
Tunisia (TN)	3	CY, MR, MT
Saudi Arabia (SA)	2	BH, KW
Fiji (FJ)	1	VU
Mauritius (MU)	1	UG
Belgium (BE)	1	LU
Switzerland (CH)	1	IT
Russia (RU)	1	AM
Slovenia (SI)	1	AL

Table 3: Foreign subsidiaries are a widespread phenomenon. 19 countries have subsidiaries with operations in 70 foreign countries, sometimes in an entirely different continent. The first column indicates the country where the state has a majority participation; the third column lists the countries where the subsidiaries operate.

	APNIC	RIPE	ARIN	AFRINIC	LACNIC	World
# companies	56	76	29	56	31	248
# countries	30	47	2	30	14	123
% countries	54	62	7	45	50	50

Table 4: State-owned Internet operators by RIR.

members have at least one state-owned network. However, most RIRs serve a large number of countries over a vast and geopolitically diverse territory (*e.g.,* RIPE comprises 76 members spanning from Northern Europe to the Middle East); in Appendix A we show a world map with all countries that have majority participation in Internet operators.

The ability to identify foreign subsidiaries is an important feature of our dataset. We find this phenomenon is broad and touches every continent. Table 3 shows which foreign countries (third column) host Internet operators controlled by companies owned by other nation states (first column). Sometimes these relationships cross continents.

Internet access markets. We provide a more detailed geographic perspective of state-ownership, nationally and abroad, in the heatmap in Figure 1, where we look at (an approximation[6] of) Internet access market footprint. Here, for each country we calculate two numbers:

- (*blue*) The maximum between *(i)* the fraction of address space geolocated in the country that is originated through BGP by ASes owned by the same country and *(ii)* the fraction of eyeballs (according to APNIC Eyeballs dataset) associated with ASes owned by the same country.
- (*green*) The same calculation as the previous point but considering ASes owned by *other* countries.

We then select the maximum between these two numbers and color the country on the map accordingly. We find that state ownership is a phenomenon much more prevalent in Africa and Asia. In addition, in a large number (12) of African countries, operators owned by other states have a significant footprint (>5%). Specifically, in 6 of these 12 countries, our estimates suggest that foreign state-owned providers hold more than 50% of the access market. Australia is another interesting case, where Singapore's SingTel operates Optus (AS7474), one of the major providers in the country (we estimate a footprint of 18.2%).

We show the fraction of network-access markets controlled by domestic, state-owned ASes in Figure 4 (data from June 2020). These numbers reveal a significant participation of many states in their network-access markets: the state's footprint is greater than 50% of IP addresses in 49 countries. The same is true for the share of eyeballs in 42 countries. Furthermore, we find 13 and 14 countries by IP address space and eyeballs, respectively (18 countries after combining both groups) where the state footprint on access networks is over 90%. We investigated whether this phenomenon is mostly related to the size of the country in terms of land or population, but we find that only 5 of these countries have fewer than 1M people. We list these 18 countries in the Appendix F and we will publish—upon paper acceptance—the full data for each country on a dedicated website.

Interestingly, the fraction of the address space originated by state-owned ASes in AFRINIC's countries is the largest out of all the regions; AFRINIC also has the largest presence of foreign state-owned ASes. In the African continent, Ooredoo and Etisalat operate multiple subsidiaries with important market shares in various countries. Conversely, in the LACNIC region, where half of the countries have state-owned ASes, the fraction of countries' address space originated by state-owned ASes is quite small. Exceptions include Cuba, Uruguay, Venezuela and Costa Rica, where state-owned providers originate 90%, 90%, 65% and 80% of the address space. We investigate LACNIC's address space and find that Brazil, Argentina and Colombia—the first (153M), third (23.8M) and the

[6]We use the fraction of IP addresses—geolocated at country-level—and of estimated eyeballs as proxies for the fraction of Internet access market in each country.

ASN-ASname	Country (cc)	cust. cone
7473-SingTel	Singapore (SG)	4235
12389-Rostelecom	Russia (RU)	3778
20485-TTK	Russia (RU)	3171
37468-Angola Cables	Angola (AO)	1843
262589-Internexa	Colombia (CO)	1315
4809-China Telecom	China (CN)	1134
3303-Swisscom	Switzerland (CH)	702
20804-Exatel	Poland (PL)	699
10099-China Unicom	China(CN)	595
132602-BSCCL	Bangladesh (BD)	556

Table 5: Ten largest customer cones of state-owned ASes (June 2020).

fourth (19M) large address spaces in Latin-America—do have state-owned providers but these operators primarily offer transit services: Telebras (AS53237), ARSAT (AS52361) and Internexa (AS18678).

Transit connectivity market. Next, we investigate the the presence of the state-owned ASes in the Internet-wide transit ecosystem. Table 5 displays the 10 largest customer cones of state-owned ASes using CAIDA's ASRank data from June 2020. We note that some state-owned providers serve transit to a large number of ASes in their customer cone (*i.e.,* they have a relevant role in terms of connectivity) and that this phenomenon is not limited to one continent but happens in 4 of the 5 RIRs. We note some differences among these operators. Some of them have clearly a large international footprint: SingTel (AS7473), Angola Cables (AS37468) and China Telecom (AS4809) operate large networks that include submarine cables. By contrast, the Russian transit networks Rostelecom (AS12389) and TTK (AS20485) mostly serve the domestic market. Similarly, Internexa's subsidiary in Brazil (AS262589) mostly provides transit services to client within Brazil.

We also identify, among the state-owned ASes, those with the fastest growing customer cones during the past decade. To that end, we compute a temporal-linear regression based on CAIDA's ASRank data. In the top-10 we identify two interesting cases: Angola Cables (AS37468) and BSCCL (AS132602), two state-owned submarine cable networks in developing countries—Angola and Bangladesh[7]. Figure 5 shows the growth of their customer cones from January 2010 to June 2020. The establishment of these companies and the deployment of their submarine cable networks were the response of the respective governments to the limited international connectivity of these countries [16, 45].

9 LIMITATIONS

Scale. We manually investigate the company structure of thousands of telcos, however, due to the size of the Internet our research only covered a fraction of the network operators. We believe our dataset includes the largest state-owned access and transit ASes, but it is less likely to capture small state-owned telecom companies. We note that our 5% threshold for IP addresses and eyeballs is not uniformly applied, because non-technical sources such as Freedom House often do not include information regarding a state-owned company's market share. Therefore, it is possible that we included in our dataset companies with a market footprint smaller than our 5% threshold. Another limitation of our approach is that non-technical sources provide us data at a company level, which makes it difficult to quantify the sources' coverage in terms of number of ASes.

Visibility and data interpretation. We rely on online resources to confirm state participation in telecom companies which limits our inference to companies whose ownership is reported online by their own resources (e.g., websites, company's annual reports) or by authoritative third-party resources (e.g., World Bank's report repository). Our interpretation of these sources might also result in inaccuracies. This is exacerbated by our limited expertise (as computer scientists) in the fields of economics and law, given that many of the reports we study are long and complex. Our direct personal experience is also mostly limited to countries in Europe and the Americas, potentially causing us to miss crucial local context. These issues may cause both false positives and false negatives in state ownership. However, our discussions with experts revealed no such inaccuracies.

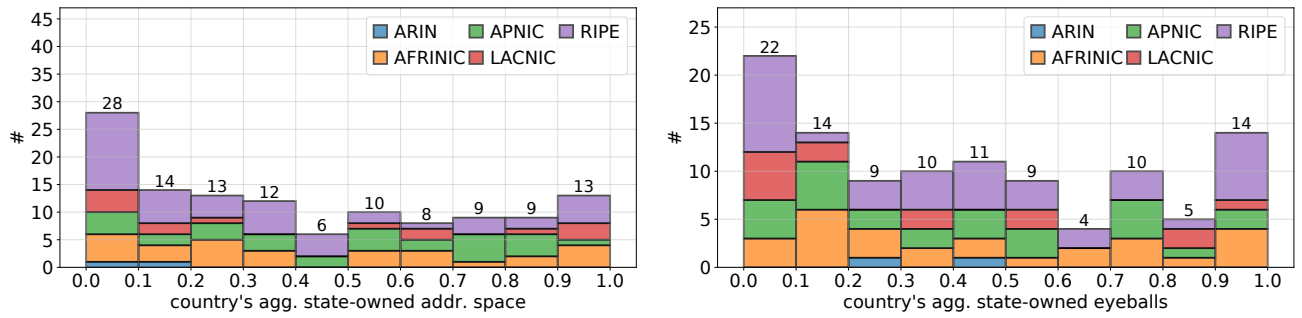
Another factor with a potential impact on our visibility is ICT adoption, as that is reflected in the number of online resources reporting state-owned enterprises (SOEs) [49]. Authoritative documents released by local institutions and websites reporting state ownership of companies are more likely to be available in countries with more mature digital ecosystems. Although this may restrict our view of a country, in this paper, we also include data from international bodies which often cover countries with presumably less mature digital ecosystems.

Misleading Company Names. Company names are central in our process of identifying state control of ASes. Misleading company names are a potential source of inaccuracies, *e.g.,* outdated names after privatizations and nationalizations. For example, the government of Fiji nationalized Vodafone Fiji in 2014 [30] but the company name has not changed. A reasonable observer might conclude, incorrectly, that the company belongs to Vodafone (a private congolomerate) when it is actually controlled by Fiji.

Changes in ownership over time. As we discussed in § 2, ownership structure is dynamic. As a consequence, our list would require maintenance to keep up to date. While conducting our study, we noted that privatizations are relatively rare. Another type of event that could impact the content of the list in the future is the birth of new state-owned providers. Moreover, in the future, some state-owned companies may break into new markets creating new foreign subsidiaries. In such cases, new state-owned companies or foreign subsidiaries will have to be incorporated into the list. We leave for future work a systematic study regarding the churn of Internet providers' ownership by states.

We believe that our dataset provides a valuable seed for (recurring) future work in this area: confirming the current validity of our list would be significantly less taxing than generating the initial list. For this paper, our manual inspection process took a single person approximately 4.6 months: 2.8 months for *technical sources* (1.6 months for Country-level AS geolocation, 1 month for APNIC eyeballs dataset, one week for Countries' main upstream

[7]We verified that these 2 ASes were owned by their respective states for the entire decade.



(a) Countries' address space **(b) Countries' eyeballs**

Figure 4: Aggregated footprint of all state-owned ASes in their home countries in terms of address space and eyeballs.

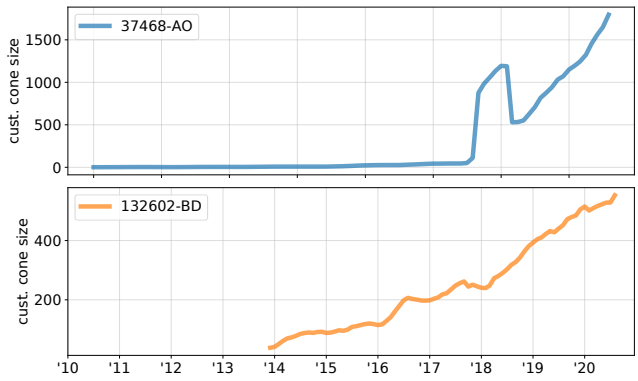


Figure 5: Growing pace of the customer cones of Angola Cables (AS37468) and BSCCL (AS132602) in the past decade.

providers) and 1.8 months for *non-technical sources* (0.8 months for Wikipedia/Freedom House and 1 months for Orbis).

Subsequently, future studies would expand the list to introduce nationalizations and known company expansions, which year by year is likely to be fractional in size compared with the preceding year's aggregate list. In the future we will try to expand this research into a cooperative project in which volunteers, from any community, could audit and suggest updates to our dataset. Making the dataset publicly available will also help with soliciting feedback.

Further, we only have evidence that the state ownership of the ASes we found in this research is valid for the reference timeframe we mention in § 3. Our list of state-owned companies does not capture companies that were state-owned at some point in the past but then were privatized (*e.g.,* Telecom Italia [40]). Moreover, the current data structure of our list does not report since when a company is under state control. Expanding the list with a field for timestamps would allow researchers to conduct more precise longitudinal analyses.

Language. We confirm the state ownership of a company by manually studying authoritative documents. Globally investigating state ownership of providers, then, might involve documents in many languages. However, in applying our methodology we noticed that the vast majority of such sources—including company websites and reports—have versions in English or Spanish. International organizations such as the IMF also publish reports primarily in English. However, we acknowledge that our view of some countries could have been compromised if for some of their companies the documents in English or Spanish we accessed were not sufficiently detailed.

10 RELATED WORK

Previous research efforts also shared the goal of classifying ASes but most are focused on classifying *all* ASes on the Internet and on assigning categories designed for purposes that are different from our study (*e.g.,* role in the AS-level Internet topology). Dhamdhere *et al.* [26] use decision trees to classify ASes—based on their peering and customer degree—into *enterprise customers, small transit providers, large transit providers, and content/hosting/access providers.* A similar study by Dimitropoulos *et al.* [28] also apply machine learning to the problem of classifying ASes using RIR registration and routing data. Wahlisch *et al.* [82] present a classification of the economic purpose of ASes in Germany by extending a taxonomy created by the German Government, and using partially-verified assignment using keyword search on AS names, descriptions, and address fields. The verification is by manual inspection.

In the Internet measurement literature, some studies leveraged the concept of state-owned Internet operator to better analyze events and extract insight: Focusing on Internet censorship, Dainotti *et al.* [24] and Raman *et al.* [62] analyzed the role of state-owned providers in country-wide Internet connectivity shutdowns and interception of HTTPS traffic, respectively. Carisimo *et al.* [19] argued the absence or lack of development of IXP in Latin American countries with almost concentrated Internet markets in the hands of state-owned ISPs. Fontugne *et al.* [31] studied the structure of the Internet in Crimea noting the role of Russian state-owned operators providing connectivity to the region.

11 CONCLUSIONS & DISCUSSION

In this paper we proposed a novel methodology to identify state-owned ASes of Internet operators using multiple and varied data sources, including both technical and non-technical sources. We found that each data source provides a unique contribution to the identification process, which indicates that our approach is well

conceived but also highlights the challenging nature of the problem and the possibility that false negatives are still present.

We have also learned about the various shortcomings and limitations of a prominent commercial business information database when utilized for this research problem. Interestingly, we would have not detected some influential transit providers neither through this database or the other input sources if we did not specifically include in our input a selection of transit operators.

Through our method we identified 989 state-owned ASes, including 193 foreign subsidiaries, from 123 and 18 countries, respectively. We discovered a higher prevalence of state-owned companies across Africa and Asia. In addition, when considering IP addresses and eyeballs as rough estimates of Internet access market share, we found that in 18 countries state-owned operators hold at least 90% of the estimated access market in their home countries. Interestingly, we also found that in 12 African countries, foreign subsidiaries hold a larger share of the access market than the country's state-owned ASes (if they were to have one). Moreover, in 6 out of these 12 countries, foreign subsidiaries originate more than 50% of the estimated access market.

As a result of applying our methodology, this work also contributes a new publicly available data set containing the state-owned organizations and ASes we have identified, as well as additional metadata reporting confirmation sources and flags identifying foreign subsidiaries. In addition, this paper contributes a new dimension to the broader topic of AS classification.

We hope that this work and the associated data set will inspire and enable a broad set of Internet measurement studies and interdisciplinary research. For example this data could be correlated with evidence about network interference for state-sponsored censorship or surveillance. Topological studies could better understand the role of autocratic governments in shaping the national Internet infrastructure. Moreover, this data could also help gaining new insight about the digital divide, often seen as a problem of infrastructure deployment in rural and urban communities [7, 15, 36, 58, 59, 64, 77]. In many countries the government's response to digital divide and specifically lack of Internet infrastructure is investing in state-owned operators. Our data set of state-owned providers could be a valuable resource to comprehensively track and measure the impact of governments' policy, for example to understand whether more ASes located in remote non metropolitan areas appear in the customer cone of state-owned providers.

12 ACKNOWLEDGEMENTS

This study was supported in part by the National Science Foundation, Grant No. 1705024. Author Gamero-Garrido was supported in part by the Microsoft Research Dissertation Grant (2019).

REFERENCES

[1] 2020. RIPE Routing Information Service (RIS). https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris. (2020).
[2] 2020. RouteViews. http://www.routeviews.org/routeviews/. (2020).
[3] Anonymous Authors. 2021. Quantifying Nations' Exposure to Traffic Observation and Selective Tampering. In *(Concurrent submission) ACM SIGCOMM Conference on Internet Measurement (IMC '21)*. ACM, New York, NY, USA, 13.
[4] World Bank. 2021. ANGOLA: SYSTEMATIC COUNTRY DIAGNOSTIC. CREATING ASSETS FOR THE POOR. https://openknowledge.worldbank.org/bitstream/handle/10986/31443/angola-scd-03072019-636877656084587895.pdf. (2021).
[5] World Bank. 2021. Case Study on the Employees Provident Fund of Malaysia. http://documents1.worldbank.org/curated/en/197861540400101962/pdf/131289-WP-WorldBankReport-PUBLIC.pdf. (2021).
[6] World Bank. 2021. CORPORATE GOVERNANCE COUNTRY ASSESSMENT: Malaysia. http://documents1.worldbank.org/curated/en/216211468088741775/pdf/908220ROSC0Box0laysia0201200PUBLIC0.pdf. (2021).
[7] Karine Barzilai-Nahon. 2006. Gaps and bits: Conceptualizing measurements for digital divide/s. *The information society* 22, 5 (2006), 269–278.
[8] Sebastian Beer and Jan Loeprick. 2015. Profit shifting: drivers of transfer (mis) pricing and the potential of countermeasures. *International Tax and Public Finance* 22, 3 (2015), 426–451.
[9] Amanah Raya Berhad. 2021. Corporate Information. https://www.amanahraya.my/profile/. (2021).
[10] Khazanah Nasional Berhad. 2021. About Us. https://www.khazanah.com.my/who-we-are/about-us/. (2021).
[11] Telekom Malaysia Berhad. 2021. Capital Structure. https://tm.listedcompany.com/capital_structure.html. (2021).
[12] BICS. 2021. Proximus acquires full ownership of BICS, securing the flexibility to execute the development and growth path of BICS and TeleSign. https://bics.com/news/proximus-acquires-full-ownership-of-bics-securing-the-flexibility-to-execute-the-development-and-growth-path-of-bics-and-telesign/. (2021).
[13] Nicholas Bloom, Aprajit Mahajan, David McKenzie, and John Roberts. 2010. Why do firms in developing countries have low productivity? *American Economic Review* 100, 2 (2010), 619–23.
[14] Bradley Huffaker and Marina Fomenkov and kc claffy. 2011. Geocompare: a comparison of public and commercial geolocation databases - Technical Report. Cooperative Association for Internet Data Analysis (CAIDA), May 2011. (2011).
[15] Francesco Bronzino, Nick Feamster, Shinan Liu, James Saxon, and Paul Schmitt. 2021. Mapping the Digital Divide: Before, During, and After COVID-19. *During, and After COVID-19 (February 17, 2021)* (2021).
[16] Angola Cables. 2021. COMPANY PROFILE. https://www.angolacables.co.ao/wp-content/uploads/2020/08/RC_Angola-Cables-2013_EN-1.pdf. (2021).
[17] Xue Cai, John Heidemann, Balachander Krishnamurthy, and Walter Willinger. 2010. Towards an AS-to-organization map. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. 199–205.
[18] CAIDA. 2021. Inferred AS to Organization Mapping Dataset. https://www.caida.org/data/as-organizations/. (2021).
[19] Esteban Carisimo, Julián M Del Fiore, Diego Dujovne, Cristel Pelsser, and J Ignacio Alvarez-Hamelin. 2020. A first look at the Latin American IXPs. *ACM SIGCOMM Computer Communication Review* 50, 1 (2020), 18–24.
[20] commsupdate. 2021. About. https://www.commsupdate.com/about/. (2021).
[21] commsupdate. 2021. MVNO Monday: a guide to the weekâĂŹs virtual operator developments. https://www.commsupdate.com/articles/2019/08/05/mvnomonday-a-guide-to-the-weeks-virtual-operator-developments/. (2021).
[22] Telegeography's commsupdate. 2021. Angola Telecom finishes restructuring ahead of privatisation. https://www.commsupdate.com/articles/2019/10/10/angola-telecom-finishes-restructuring-ahead-of-privatisation/. (2021).
[23] Alberto Dainotti, Karyn Benson, Alistair King, Bradley Huffaker, Eduard Glatz, Xenofontas Dimitropoulos, Philipp Richter, Alessandro Finamore, and Alex C Snoeren. 2016. Lost in space: improving inference of IPv4 address space utilization. *IEEE Journal on Selected Areas in Communications* 34, 6 (2016), 1862–1876.
[24] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. 2011. Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. 1–18.
[25] Oficina de Planeamiento y Presupuesto del Uruguay. 2021. Portal de Transparencia Presupuestaria. https://transparenciapresupuestaria.opp.gub.uy/inicio/empresas-públicas. (2021).
[26] Amogh Dhamdhere and Constantine Dovrolis. 2008. Ten Years in the Evolution of the Internet Ecosystem. In *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement (IMC '08)*. ACM, New York, NY, USA, 183–196. https://doi.org/10.1145/1452520.1452543
[27] Digital Element. 2021. NetAcuity. https://www.digitalelement.com/solutions/. (2021).
[28] X. Dimitropoulos, D. Krioukov, G. Riley, and k. claffy. 2006. Revealing the Autonomous System Taxonomy: The Machine Learning Approach. In *Passive and Active Network Measurement Workshop (PAM)*. PAM 2006, Adelaide, Australia.
[29] KWSP EPF. 2021. Organisation Structure: Board Members. https://www.kwsp.gov.my/about-epf/corporate-profile/organisation-structure#boardMembers. (2021).
[30] Vodafone Fiji. 2021. About Vodafone Fiji. https://www.vodafone.com.fj/about/about-us. (2021).
[31] Romain Fontugne, Ksenia Ermoshina, and Emile Aben. 2020. The Internet in Crimea: a Case Study on Routing Interregnum. In *2020 IFIP Networking Conference (Networking)*. IEEE, 809–814.
[32] Association francaise pour le nommage Internet. 2021. https://www.afnic.fr/en/. (2021).

[33] Tina Freyburg and Lisa Garbe. 2018. Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa. *International Journal of Communication* 12 (2018), 3896–3916.

[34] International Monetary Fund. 2014. GOVERNMENT FINANCE STATISTICS MANUAL 2014. https://www.imf.org/external/Pubs/FT/GFS/Manual/2014/gfsfinal.pdf. (2014).

[35] International Monetary Fund. 2020. STATE-OWNED ENTERPRISES: THE OTHER GOVERNMENT. https://www.imf.org/~/media/Files/Publications/fiscal-monitor/2020/April/English/ch3.ashx. (2020).

[36] Bjørn Furuholt and Stein Kristiansen. 2007. A rural-urban digital divide? Regional aspects of Internet use in Tanzania. *The Electronic Journal of Information Systems in Developing Countries* 31, 1 (2007), 1–15.

[37] Peter N Gal. 2013. Measuring total factor productivity at the firm level using OECD-ORBIS. (2013).

[38] Alexander Gamero-Garrido. 2021. *Transit Influence of Autonomous Systems: Country-Specific Exposure of Internet Traffic.* Ph.D. Dissertation. UC San Diego.

[39] Gharaibeh, Manaf and Shah, Anant and Huffaker, Bradley and Zhang, Han and Ensafi, Roya and Papadopoulos, Christos. 2017. A look at router geolocation in public and commercial databases. In *ACM Internet Measurement Conference (IMC)*.

[40] Andrea Goldstein. 2003. Privatization in Italy 1993-2002: Goals, institutions, outcomes, and outstanding issues. *Institutions, Outcomes, and Outstanding Issues (April 2003)* (2003).

[41] Etisalat Group. 2021. 2020 Etisalat Group Annual Report (page 46). https://etisalat.com/en/system/com/assets/docs/annual-report/2020/en-2020-etisalat-group-annual-report.pdf. (2021).

[42] Freedom House. 2019. Freedom of the 2019: Uzbekistan. https://freedomhouse.org/country/uzbekistan/freedom-net/2019. (2019).

[43] Freedom House. 2021. Freedom of The Net: Angola 2018. https://freedomhouse.org/country/angola/freedom-net/2018. (2021).

[44] Harry Huizinga and Luc Laeven. 2008. International profit shifting within multinationals: A multi-country perspective. *Journal of Public Economics* 92, 5-6 (2008), 1164–1182.

[45] Faheem Hussain. 2011. ICT sector performance review for Bangladesh. *Available at SSRN 2013707* (2011).

[46] Geoff Huston. 2014. How Big is that Network? https://labs.apnic.net/?p=526. (2014).

[47] ICANN. 2013. 2013 Registrar Accreditation Agreement. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy. (2013).

[48] Sebnem Kalemli-Ozcan, Bent Sorensen, Carolina Villegas-Sanchez, Vadym Volosovych, and Sevcan Yesiltas. 2015. *How to construct nationally representative firm level data from the Orbis global database: New facts and aggregate implications.* Technical Report. National Bureau of Economic Research.

[49] Raul Katz and Fernando Callorda. 2018. Accelerating the development of Latin American digital ecosystem and implications for broadband policy. *Telecommunications Policy* 42, 9 (2018), 661–681.

[50] Loet Leydesdorff and Ping Zhou. 2014. Measuring the knowledge-based economy of China in terms of synergy among technological, organizational, and geographic attributes of firms. *Scientometrics* 98, 3 (2014), 1703–1719.

[51] Moody's. 2021. Moody's Completes Acquisition of Bureau van Dijk. https://ir.moodys.com/news-and-financials/press-releases/press-release-details/2017/Moodys-Completes-Acquisition-of-Bureau-van-Dijk/default.aspx. (2021).

[52] The Government of Sweden. 2021. State-owned enterprises. https://www.government.se/government-policy/state-owned-enterprises/. (2021).

[53] Prime Minister's Office. 2021. State majority-owned companies . https://vnk.fi/en/state-majority-owned-companies. (2021).

[54] Orange. 2021. Consolidated financial statements 2019. https://www.orange.com/sirius/derniers_resultats/en/Consolidated%20financial%20statements%202019.pdf. (2021).

[55] The Number Resource Organization. 2021. Regional Internet Registries. https://www.nro.net/about/rirs/. (2021).

[56] Alberto Osnago, Nadia Rocha, and Michele Ruta. 2017. Do deep trade agreements boost vertical FDI? *The World Bank Economic Review* 30, Supplement_1 (2017), S119–S125.

[57] PeeringDB. 2021. PeeringDB. https://www.peeringdb.com. (2021).

[58] Lorna Philip, Caitlin Cottrill, John Farrington, Fiona Williams, and Fiona Ashmore. 2017. The digital divide: Patterns, policy and scenarios for connecting the âĂŸfinal fewâĂŹin rural communities across Great Britain. *Journal of Rural Studies* 54 (2017), 386–398.

[59] Lorna J Philip, Caitlin Cottrill, and John Farrington. 2015. âĂŸTwo-speedâĂŹScotland: Patterns and implications of the digital divide in contemporary Scotland. *Scottish Geographical Journal* 131, 3-4 (2015), 148–170.

[60] Ingmar Poese, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP Geolocation Databases: Unreliable? *SIGCOMM Comput. Commun. Rev.* 41, 2 (April 2011), 5356. https://doi.org/10.1145/1971162.1971171

[61] PTCL. 2021. PTCL Annual Report (page 233). https://ptcl.com.pk/uploads/Annual%20Report-2020.pdf. (2021).

[62] Ram Sundara Raman, Leonid Evdokimov, Eric Wurstrow, J Alex Halderman, and Roya Ensafi. 2020. Investigating Large Scale HTTPS Interception in Kazakhstan. In *Proceedings of the ACM Internet Measurement Conference*. 125–132.

[63] Francesco Rosati and Lourenço Galvão Diniz Faria. 2019. Business contribution to the Sustainable Development Agenda: Organizational factors related to early adoption of SDG reporting. *Corporate Social Responsibility and Environmental Management* 26, 3 (2019), 588–597.

[64] Koen Salemink, Dirk Strijker, and Gary Bosworth. 2017. Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in rural areas. *Journal of Rural Studies* 54 (2017), 360–371.

[65] SEC. 2021. LIST OF CERTAIN SUBSIDIARIES OF AMERICA MOVIL, S.A.B. DE C.V. https://www.sec.gov/Archives/edgar/data/1129137/000119312511138519/dex81.htm. (2021).

[66] Justine Sherry, Shaddi Hasan, Colin Scott, Arvind Krishnamurthy, Sylvia Ratnasamy, and Vyas Sekar. 2012. Making middleboxes someone else's problem: Network processing as a cloud service. *ACM SIGCOMM Computer Communication Review* 42, 4 (2012), 13–24.

[67] SingTel. 2021. Annual Report 2019. https://cdn.aws.singtel.com/annualreport/2019/files/Singtel-AR2019-FULL_LR.pdf. (2021).

[68] SingTel. 2021. Singtel to subscribe to Bharti AirtelâĂŹs rights issue. https://cdn.aws.singtel.com/annualreport/2019/files/Singtel-AR2019-FULL_LR.pdf. (2021).

[69] Congo Telecom. 2021. About. http://www.congotelecom.cg/about.html. (2021).

[70] China Telecom. 2021. China Telecom Will Achieve 800M Complete Coverage, Launch Pre-commercial VoLTE in 2017. https://www.ctamericas.com/china-telecom-to-achieve-800m-complete-coverage-launch/. (2021).

[71] Telegeography. 2021. Comcel board approves Telmex Colombia stake purchase. https://www.commsupdate.com/articles/2010/12/30/comcel-board-approves-telmex-colombia-stake-purchase/. (2021).

[72] Telegeography. 2021. GlobalComms Database Service. https://www2.telegeography.com/globalcomms-database-service. (2021).

[73] Deutsche Telekom. 2021. Shareholder structure. https://www.telekom.com/en/investor-relations/company/shareholder-structure. (2021).

[74] Telia. 2021. Shareholders. https://www.teliacompany.com/en/about-the-company/corporate-governance/shareholders/. (2021).

[75] Telkomsel. 2021. 2017 Annual Report (page 47). https://www.telkomsel.com/download?type=annual&category=report&file=TSEL_AR2017_Web.pdf. (2021).

[76] the International Telecommunications Union. 2021. https://www.itu.int. (2021).

[77] Leanne Townsend, Arjuna Sathiaseelan, Gorry Fairhurst, and Claire Wallace. 2013. Enhanced broadband access as a solution to the social and economic problems of the rural digital divide. *Local Economy* 28, 6 (2013), 580–595.

[78] Ucell. 2021. About company. https://ucell.uz/en/myucell/about_company. (2021).

[79] International Telecommunications Unit. 2021. Our Mandate, Mission and Strategy. https://www.itu.int/en/ITU-D/Capacity-Building/Pages/MandateStrategy.aspx. (2021).

[80] Bureau van Dijk. 2014. Orbis Overview. https://www.bvdinfo.com/en-us/our-products/data/international/orbis. (2014).

[81] Bureau van Dijk. 2021. About us. https://www.bvdinfo.com/en-us/about-us. (2021).

[82] Wahlisch, Matthias and Schmidt, Thomas and de Brun, Markus and Haberlen, Thomas. 2012. Exposing a Nation-Centric View on the German Internet - A Change in Perspective on AS-level. In *Passive and Active Measurement Conference (PAM)*.

[83] Paul A Watters, Aaron Herps, Robert Layton, and Stephen McCombie. 2013. ICANN or ICANT: Is WHOIS an Enabler of Cybercrime?. In *2013 Fourth Cybercrime and Trustworthy Computing Workshop*. IEEE, 44–49.

A COUNTRIES WITH STATE-OWNED INTERNET PROVIDERS AROUND THE WORLD

Figure 6 shows a world's heatmap of countries having majority state-owned Internet providers (blue) and the minority state-owned Internet providers (orange) we found during our data discovery process.

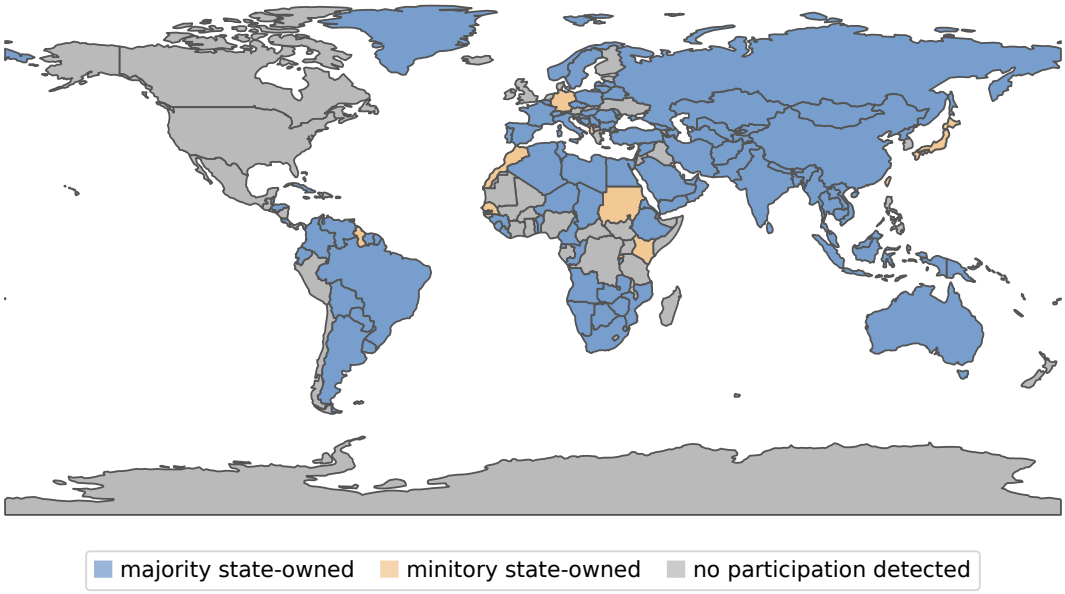


Figure 6: World map of countries having majority state-owned Internet providers (blue). Minority state-owned Internet providers found during the data discovery process are indicated in orange.

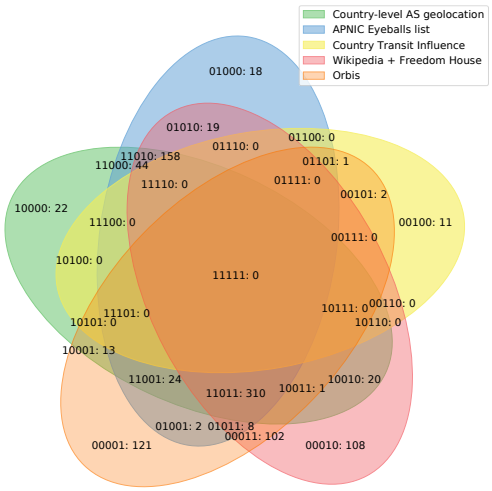


Figure 7: Venn Diagram of the contribution of each data source to the list of state-owned ASes

B INDIVIDUAL CONTRIBUTION OF EACH DATA SOURCE TO THE FINAL LIST OF STATE-OWNED ASES

Table 6 shows the individual contribution of each data source (fraction of subsidiaries in parentheses) at the end of the process. In addition, the third row indicates the number of minority state-owned that we also found with each data source.

C CONTRIBUTION AND OVERLAP OF DATA SOURCES TO THE FINAL LIST OF STATE-OWNED ASES

Figure 7 shows a Venn diagram with the contribution of each data source to the final list of state-owned ASes.

Data source	State-owned ASes	Minority state-owned
Geolocated addresses	593 (126)	253
APNIC's Eyeballs list	586 (151)	288
CTI	15 (0)	7
Wikipedia+FH	728 (126)	4
Orbis	587 (123)	0
TOTAL	984 (193)	302

Table 6: Individual contribution of each data source (fraction of subsidiaries in parentheses). Note that the total is not the sum of the rows since the individual contributions partially overlap.

Country name (cc)	ASN	AS name
Vietnam (VN)	45895	MOBIFONEGLOBAL-AS-VN
Vietnam (VN)	45896	MOBIFONEGLOBAL-AS-VN
Vietnam (VN)	45897	MOBIFONEGLOBAL-AS-VN
Bangladesh (BD)	132602	BSCCL
Cuba (CU)	11960	ETECSA
Belarus (BY)	60330	BCTBY-AS
Belarus (BY)	205475	BECLOUD-RDC-AS
Belarus (BY)	35647	BYIX-AS
Belarus (BY)	60280	NTEC

Table 7: List of state-owned ASes only covered CTI.

D STATE-OWNED ASES ONLY DISCOVERED BY CTI

Table 7 shows the list of state-owned ASes that are only captured by CTI.

E EXCLUDED STATE-FUNDED ORGANIZATIONS

Academic networks: We remove university networks and academic backbones from the candidate list. We exclude government-funded university networks (*e.g.,* Universidad de Buenos Aires-AS3449) and academic backbones (*e.g.,* Germany's DFN-AS680) from the list because we assume that governments do not uses such networks to participate and promote Internet markets. In addition, despite campus residents access to the Internet by using university networks and universities rely on academic backbones as upstream providers, none of these networks compite in general and open access and transit markets.

Governments's bureaucratic networks: We exclude all ASes providing connectivity to government offices, secretaries or any other government-dependent institutions. Again, we remove these government-funded networks since they just serve to these offices and not to the resident, for instance the State of California-AS2642 or the European Central Bank-AS31614. Another prominent example is the US DoD-AS721 announcing a customer cone of nearly 80M IP address in March 2021, however, this network only connects institutions related to the DoD.

Government's Internet administrative organizations: We exclude from the list governments organizations that support and enable the functioning of the country's Internet but do not provide Internet services such as transit or access. Some country-level organizations, for examples the Bolivian Agency for the Development of the Information Society, ADSIB-AS52250, are relevant to the country's Internet functioning since these institutions delegated Internet resources such as domain names, and sometime, prefixes and ASNs too. In other countries, this role is reserved to the NIC, which tends to have a more complex legal structures (non-profit, under university managements or multistakeholder boards) that could not be classified as state-owned. In either case, these organizations sometimes host the ccTLD serves, which is a key component in a country's Internet infrastructure. However, we exclude these organizations because they do not offer broadband subscriptions or transit services to the general public. Although these institutions are beyond the scope of this paper, we would like to acknowledge that these institutions play an important role in closing the digital divide by providing resources, knowledge and services to operators and companies in their countries.

Unrelated to Internet services: We filter out hardware manufacturers or telecommunication companies that do not provide Internet services.

F STATE-OWNED INTERNET PROVIDERS WITH MORE THAN 0.9 OF THE ESTIMATED ACCESS MARKET

Table 8 shows the list of countries (19 in total) in which our estimated Internet access market footprint of state-owned ASes is over 0.9.

Country (cc)	Approx. Internet access market footprint
Ethiopia (ET)	1.00
Tuvalu (TV)	1.00
Cuba (CU)	1.00
Greenland (GL)	1.00
Djibouti (DJ)	1.00
Syria (SY)	1.00
United Arab Emirates (AE)	0.99
Eritrea (ER)	0.99
Suriname (SR)	0.97
China (CN)	0.97
Libya (LY)	0.97
Yemen (YE)	0.97
Algeria (DZ)	0.96
Macao (MO)	0.96
Andorra (AD)	0.94
Iran (IR)	0.92
Uruguay (UY)	0.92
Turkmenistan (TM)	0.91

Table 8: Countries with over 0.9 Approx. Internet access market footprint in their home countries.

G COUNTRY-LEVEL TRANSIT INFLUENCE

The transit influence $CTI_M(AS, C) \in [0, 1]$ is calculated using a set of monitors[8] M as

$$\sum_{m \in M} \left(\frac{w(m)}{|M|} \cdot \sum_{p | \text{onpath}(AS,m,p)} \left(\frac{a(p,C)}{A(C)} \cdot \frac{1}{d(AS,m,p)} \right) \right), \quad (1)$$

where $w(m)$ is monitor m's weight, calculated as the inverse of the number of monitors available from its same AS; $\text{onpath}(AS, m, p)$ is true if AS is present on a preferred path observed by monitor m to a prefix p originated by a probed and responsive origin network, and m is not contained within AS itself; $a(p, C)$ is the number of addresses in prefix p geolocated to country C that are not covered by a more specific prefix; $A(C)$ is the total number of IP addresses

[8] A BGP monitor is an operational border router that forwards announcements to a collection database. These routers are hosted by cooperative ASes who voluntarily disclose their routing information.

geolocated to country C; and $d(AS, p, m)$ is the number of AS-level hops between AS and prefix p as viewed by monitor m. Please refer to Gamero-Garrido's doctoral dissertation [38] for a more detailed definition of the CTI metric.

Quantifying Nations' Exposure to Traffic Observation and Selective Tampering

Alexander Gamero-Garrido[1,2], Esteban Carisimo[3], Shuai Hao[4], Bradley Huffaker[1], Alex C. Snoeren[6], and Alberto Dainotti[1,5]

[1] CAIDA, UC San Diego
[2] Northeastern University
[3] Northwestern University
[4] Old Dominion University
[5] Georgia Institute of Technology
[6] UC San Diego

Abstract. Almost all popular Internet services are hosted in a select set of countries, forcing other nations to rely on international connectivity to access them. We identify nations where traffic towards a large portion of the country is serviced by a small number of Autonomous Systems, and, therefore, may be exposed to observation or selective tampering by these ASes. We introduce the Country-level Transit Influence (CTI) metric to quantify the significance of a given AS on the international transit service of a particular country. By studying the CTI values for the top ASes in each country, we find that 34 nations have transit ecosystems that render them particularly exposed, where a single AS is privy to traffic destined to over 40% of their IP addresses. In the nations where we are able to validate our findings with in-country operators, our top-five ASes are 90% accurate on average. In the countries we examine, CTI reveals two classes of networks frequently play a particularly prominent role: submarine cable operators and state-owned ASes.

1 Introduction

The goal of this study is to identify instances where a significant fraction of a country's inbound international traffic is managed by a select few networks. Such networks are in a position to observe and tamper with a nation's traffic, as could any third-parties who infiltrate them (*e.g.,* using a phishing attack or a remote vulnerability exploitation). For instance, observation—of unencrypted traffic and metadata—may be performed by domestic or foreign actors with the purpose of conducting surveillance or espionage, respectively. Conversely, selective tampering—for instance, with individual network flows carrying popular-application traffic—has been reported by actors that are both domestic (e.g., government censorship) and foreign (e.g., dis-information campaigns).

Because actual traffic information is difficult to obtain at a global scale, we instead quantify the fraction of a country's IP addresses exposed to tampering and observation by specific networks. While all IP addresses are clearly not created equal, they facilitate an apples-to-apples comparison across nations, and

the ranking of networks influencing a particular country. Traffic towards any given IP address is frequently handled by so-called transit networks, *i.e.,* those who sell connectivity to the rest of the Internet to other, customer networks for a fee; customers include consumer-serving access networks.

These transit networks are often unknown and unaccountable to end users. This opacity may allow both domestic and foreign actors to observe or tamper with traffic—capabilities we term *transit influence*—without facing diplomatic or political backlash from governments, activists or consumer groups. We aim to bring transparency to the public regarding oversized observation and tampering capabilities granted to specific transit networks in a large group of nations.

In order to reveal these crucial, nation-level topological features, we develop the country-level transit influence (CTI) metric. CTI quantifies the transit influence a particular network exerts on a nation's traffic. Studying transit influence requires an analysis of the global routing ecosystem which enables networks to exchange traffic between them. We extract information from the Border Gateway Protocol (BGP), the central system by which networks exchange interconnection information. CTI is based on an analysis of a large compendia of BGP data [54,8] and includes both topological and geographic filters designed to facilitate inference despite incomplete and biased data [48,31,25].

We apply CTI in countries that lack peering facilities such as Internet exchange points (IXPs) at which access networks might connect directly with networks of other nations. In these *transit-dominant* nations, transit networks—often a select few based in geographically distant countries [16,28,32,58]—serve as the dominant form of connectivity to the global Internet. Moreover, the lack of internationally connected, domestic co-location facilities places these nations at further risk of exposure to observation and tampering because popular content is generally hosted abroad [19,26,51,37,60].

We employ a two-stage approach based on a comprehensive set of passive inference and active measurements. First, we identify transit-dominant countries. Countries that are transit dominant may be more exposed to observation and tampering by transit providers than countries where peering agreements are prevalent: the latter can receive some traffic from other countries through such peering agreements and bypass transit providers. Second, we quantify the transit influence of the networks serving each country using the CTI methodology, the central contribution of this study. We validate our findings from both stages with in-country network operators at 123 ASes in 19 countries who each confirm that our results are consistent with their understanding of their country's networks. These discussions, and our analyses showing the metric's stability, lend confidence to our inferences despite the considerable technical challenges in this measurement space.

In addition to releasing our code and data, our contributions include:

1. A new Internet cartography metric that quantifies the transit influence a particular network exerts on a nation's traffic: the country-level transit influence (CTI) metric, which ranges over $[0, 1]$.

2. We apply CTI to infer the most influential transit networks in 75 countries that rely primarily on transit for international connectivity. These countries have, in aggregate, ≈1 billion Internet users (26% of the world [2]). We find that many of these countries have topologies exposing them to observation or tampering: in the median case, the most influential transit network manages traffic towards 35% of the nation's IP addresses.
3. We identify two classes of ASes that are frequently influential: those who operate submarine cables and companies owned by national governments.

Ethical disclaimer. We acknowledge several ethical implications of our work. Our mass (validation) survey of operators was classified as exempt by our IRB. Our reporting of available paths to repressive countries might trigger government intervention to remove such paths. Another potential issue is the identification of networks that would yield the most expansive observation or tampering capabilities in a country, which is potentially useful information for a malicious actor. We believe most governments and sophisticated attackers already have access to this information, and that our study may lead to mitigation of these concerning topological features; thus, the benefits significantly exceed the risk.

Roadmap. The remainder of this paper is organized as follows. We start in §2 with a high-level overview of our methodology before describing how we assign nationality to prefixes, ASes, and BGP vantage points (§3). We introduce the CTI metric in §4. We apply CTI in 75 countries where international connectivity is predominantly transit and describe our findings in §5. Then, we discuss in detail how we identified the transit-dominant countries (§6). We present our validation with operators and stability analyses in §7. §8 discloses some limitations of our study while §9 compares with prior work. Due to space constraints, we include further details and a flowchart summarizing our full methodology in the appendix. We release the CTI code and datasets at `https://github.com/CAIDA/mapkit-cti-code`.

2 Approach Overview

Conceptually, international Internet traffic crosses a nation's border at some physical location, likely along a link connecting two routers. For our purposes, we are not interested in the physical topology, but the logical one: in which autonomous system(s) does international traffic enter a nation on its way to access networks in that country (i.e., origin ASes). Topologically, these ASes can have two different types of relationship with the first domestic AS encountered: transit (provider-to-customer or *p2c*) or peering (peer-to-peer or *p2p*). We focus on countries where international connectivity is dominated by transit (p2c) interdomain relationships as they are easier to identify from public data sources.

High-level model. We look for evidence of a country's exposure to observation or selective tampering by specific networks. Studying this exposure requires a quantitative model of the reliance of the country's access networks, in aggregate, on specific transit networks. The model must factor in the size of the address space originated by each AS with presence in the country. Intuitively,

the greater the share of a country's IP addresses that are served by a particular transit AS, the higher the potential exposure of the nation's inbound traffic to observation or tampering by that AS. The model must then produce a country-level metric of exposure for each transit network serving the nation. To that end, we determine the frequency at which transit networks appear on routes towards the country's IP addresses.

We start our model by building a graph where nodes are ASes and edges are connections between them, weighted by address space. Then, a metric of node prominence on said graph provides a quantitative assessment of how frequently a (transit) node AS_t is traversed when delivering traffic from any given node to edge (origin) nodes. The higher the value of this metric for any AS_t in a given country, the more exposed the transit ecosystem is. At one extreme (most exposed) are countries with a single transit provider (*e.g.,* a legally-mandated monopoly) connecting every network in the country to the rest of the Internet; at the other end are countries with many transit providers, each delivering traffic to a small fraction of the nation's IPs. Note that we do not need complete visibility of the graph (*e.g.,* backup links) to infer potential exposure to observation or tampering, as traffic will likely flow through the links that are visible given capacity constraints on long-haul (incl. international) links [14,67,44,50].

Our technical approach to build this conceptual model using real data uses as inputs a combination of two types of measurements: *(i)* passive, to study AS-level connectivity, and *(ii)* active, to study transit dominance.

AS-level connectivity. We rely on two major input sources: BGP paths and prefixes from RouteViews [8] and RIPE RIS [6], and AS relationship inferences from CAIDA. We begin with the 848,242 IPv4 prefixes listed in CAIDA's Prefix-to-Autonomous System mappings derived from RouteViews [22], excluding the 6,861 (0.8%) prefixes with (invalid) length greater than 24, and the 9,275 (1.1%) originated by multiple ASes. We find those prefixes in the 274,520,778 IPv4 AS-level paths observed in BGP table dumps gathered by AS-Rank [1] from RIPE/RouteViews [8][6] during the first five days of March 2020. We consider the set of prefixes and the ASes that originate them on each observed path in combination with the 377,879 inferred AS-level relationships published by CAIDA [5].[7]

Transit dominance. Because we are focused only on countries where transit—as opposed to peering—is the main form of trans-border connectivity, we use active measurements to identify and exclude nations with evidence of foreign peering, *i.e.,* where an AS that originates addresses geolocated to the country establishes a peering agreement with another AS primarily based in another country[8]. We conduct a two-week-long active measurement campaign (see

[7] In the 75 countries where we study transit influence, no path contained any of: unallocated ASes, loops, poisoned paths (where a non-clique AS is present between two clique ASes, clique being the AS-level core of the Internet inferred by [5]); additionally, all paths towards these countries are seen at least once per day across all five days.

[8] This "nationality" assignment is described in Sec. 3.

Sec. 6.2) in May 2020 to determine which countries are transit dominant based on the business relationship between the "border" ASes traversed by our probe packets while entering the country (as inferred by BdrmapIT [49]).

3 Definitions of Nationality

CTI hinges on the correct nationality assignment for IP address prefixes and BGP monitors. ASes are also assigned a nationality in the transit-dominance analysis. Given the diverse set of information available, we devise distinct methods for each. (We include an analysis of CTI stability given an alternative geolocation input in §7). For our purposes, a country is one of the 193 United Nations member states, either of its two permanent non-member observer states, or Antarctica.

Address prefixes. We first geolocate each IP address in every observed BGP prefix to a country using Netacuity [12]. Then, on a country-by-country basis, we count how many addresses in each prefix are geolocated to that country. If the number is less than 256 (a /24), we round up to 256. If Netacuity does not place any of a prefix's IP addresses in a country, we attempt to find a delegation block from the March 2020 RIR delegation files [7] that covers the entirety of the prefix. If there is one we assign all of the delegated prefix's addresses to the indicated country. Hence, while Netacuity can place a prefix in multiple countries, at most one country will receive addresses through the RIR process, and only if it was not already associated with the prefix through Netacuity. Netacuity accounts for 95.1% of all prefix-to-country mappings, while delegation-derived geolocation accounts for the rest.

A particularly pressing concern with geolocation is the correct assignment of IP addresses belonging to large transit ASes with a presence in many countries. We compute the fraction of a country's address space that is originated by ASes that have at least two thirds of their addresses in that country. In the vast majority of countries, the address space is dominated by ASes that are primarily domestic.

BGP monitors. As our study is focused on measuring inbound country-level connectivity, we seek to limit our analysis to paths going towards addresses in the target country from a BGP monitor located outside that country. Hence, we confirm the BGP monitor locations listed by RouteViews [59] and RIPE RIS [57] through a set of active measurements. The details of this process are included in Appendix A.

Autonomous Systems. Our transit dominance analysis relies on a concept of AS nationality, which is based on IP geolocation of the AS' originated addresses; for transit providers, we also include the IP addresses originated by direct customers. We classify each autonomous system AS operating in a country C as being *domestic*, $AS \in \mathrm{dom}(C)$, when the AS has at least two thirds of its addresses in the country, and *foreign* otherwise. The vast majority (97.4%) of ASes are classified as domestic in one country, with the remaining small fraction being classified as foreign in every country. In fact, 89.8% of ASes have all of

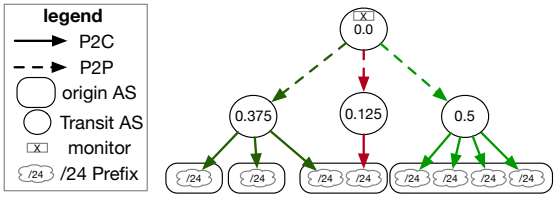


Fig. 1: Example of Country-Level Transit Influence.

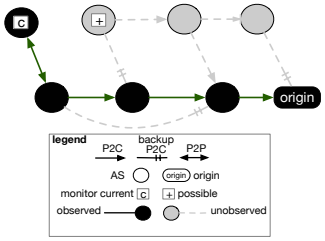


Fig. 2: Unobserved paths in BGP.

their address in a single country, and 98.6% have a strict majority of addresses in one country.

4 Transit Influence Metric

We define the transit influence $CTI_M(AS, C) \in [0, 1]$ using a set of BGP monitors M as

$$\sum_{m \in M} \left(\frac{w(m)}{|M|} \cdot \sum_{p | \text{onpath}(AS,m,p)} \left(\frac{a(p,C)}{A(C)} \cdot \frac{1}{d(AS,m,p)} \right) \right), \tag{1}$$

where $w(m)$ is monitor m's weight (Sec. 4.1) among the set of monitors (Sec. 4.2); $\text{onpath}(AS, m, p)$ is true if AS is present on a preferred path observed by monitor m to a prefix p, and m is not contained within AS itself (Sec. 4.2); $a(p, C)$ is the number of addresses in prefix p geolocated to country C; $A(C)$ is the total number of IP addresses geolocated to country C; and $d(AS, p, m)$ is the number of AS-level hops between AS and prefix p as viewed by monitor m (Sec. 4.1).

We illustrate CTI's use in Fig. 1, with CTI values for a toy example with three transit ASes and four origin ASes, in a country with eight /24 prefixes: the transit AS on the right has the highest CTI, since it serves the most addresses (half of the country), followed by the transit AS on the left (3/8) and the AS in the center (1/8). Note that the top AS has a CTI of 0, because it hosts the BGP monitor from which the set of routes used in this toy example are learned—hence, $\text{onpath}(AS_t, m, p)$ is always false for that AS. Should that AS not be the host of the BGP monitor (or be seen on these routes through another monitor), it would have a CTI of 0.5—transit influence over the entire country as an indirect transit provider (distance 2 from the prefixes).

Note that originating addresses directly does not grant an AS transit influence, as our focus is on identifying ASes that carry traffic to destinations outside of their network.

4.1 CTI components

We explain the rationale for the various factors in Eq. 1 in the following subsections.

Indirect transit discount. As the number of AS-level hops from the origin increases, so too does the likelihood that there exist alternative paths towards the same origin AS of which we have no visibility (*e.g.,* backup links, less-preferred paths). Fig. 2 shows this limitation in visibility for a toy example with a single origin AS. There, given the location of BGP monitor C we see the AS-level chain in black, erroneously concluding that the origin AS has a single direct transit provider and two indirect transit providers. In reality, there exists another set of both direct and indirect transit providers (the AS-level chain in light gray). We miss all these paths given that we do not have a monitor in any neighbor of a light-gray AS (such as that marked with a plus sign). In this example we miss backup links of the origin AS, as well as preferred links of the origin's direct transit provider, and a backup link of both indirect transit providers.

As a coarse mechanism aimed at mitigating this limited visibility, we discount the influence of transit providers in proportion to the AS-level distance from the origin: we apply a discount factor as $1/1, 1/2, ..., 1/k$, where k is the number of AS-level hops from the origin AS. In practice, that means we do not discount the measurements of direct transit providers, as there the probability of missing a backup or less-preferred link is lowest. We note that this heuristic yields a conservative estimate of the observation opportunities of an indirect transit provider over traffic flowing towards a country.

Prioritizing AS diversity. ASes can host more than one BGP monitor. In fact, more than 20 ASes in RIPE RIS and RouteViews host multiple monitors; for instance, AS3257-GTT hosts five. In order to favor a topologically-diverse view (given the available observations), if more than one monitor from the same AS sees an announcement for the same prefix, we discount their observations to limit the influence of monitor ASes with multiple monitors. Formally, the weight for each monitor m's observation of a prefix is $w(m) = 1/n$, where n is the number of BGP monitors in the AS that see an announcement of that prefix.

4.2 Filtering ASes

To correct for the limited, non-uniform coverage of the BGP monitors that collect our table dumps, we apply a number of filters to the set of paths over which we compute CTI.

Provider-customer AS filter. BGP monitors by definition collect paths from the AS hosting the monitor to the origin AS. Therefore, we always exclude the AS hosting the BGP monitor from the path to avoid inflating their transit influence. Further, we employ a heuristic that attempts to consider only the portion of the path relevant to the origin prefix, and ignore the portion dictated by the monitor's topological location.

The intuition behind our filter is that, from the perspective of the origin AS, there is a "hill" above it capped by the last observed provider-customer (p2c, *i.e.,* transit) link, with traffic flowing from the hill's peak down towards

the origin. The transit AS in that link is the highest point in the path we want to keep, as it directs traffic towards its customer (and its customer's customers, if applicable). After reaching that topological peak, we discard any other AS present in the path. The remaining path would then include the origin AS, its direct or indirect transit provider at the topological peak, and any other ASes appearing between the origin AS and the direct or indirect transit provider. Note that this filter excludes peers of the transit provider at the peak—appearing between the topological peak and the AS hosting the BGP monitor—since we only apply CTI in transit-dominant countries, and therefore these peers are unlikely to be central to the country's connectivity.

Formally, for the analysis presented in this paper, we refine $\text{onpath}(AS_t, m, p)$ to be true only if the path observed at monitor m has at least one inferred p2c link where the customer is either the origin of p or closer to it than AS_t, *i.e.,* we discard paths where there is no topological peak from the perspective of the origin. This heuristic discards 0.2% of the paths observed by our monitors. In the median country we discard 0.2% of paths using this filter, with 0.3% being the average case. In all countries we keep over 98.6% of paths.

This filter ensures that at least one AS (the inferred customer of the transit AS) relies on at least one other AS (the inferred transit provider) for transit from and towards the core of the Internet. As we aim to measure transit influence, these business relationships are an important source of information: merely being directly connected to an AS path that reaches the origin AS in a given country does not necessarily make an AS influential; being a direct provider of the origin, or of an AS closer to the origin, lends more confidence to our inference of influence[9].

CTI outlier filtering. Finally, we filter BGP-monitor-location noise by removing outlier estimates of transit influence—both overestimates and underestimates resulting from the AS hosting a BGP monitor being topologically too close or too far from the origin AS—to get an accurate assessment of transit influence towards that origin. We implement a filter recently proposed for another AS-topology metric (AS hegemony [31], see §9). Specifically, we compute the CTI of each transit provider AS_t using BGP monitors from each monitor-hosting AS_h independently, as $CTI_{m(AS_h)}(AS_t, C)$, where $m(AS_h)$ is the set of monitors within AS_h. We determine which potentially-biased AS_h have gathered observations producing $CTI_{m(AS_h)}(AS_t, C)$ values in the bottom and top 10% of all values for that transit provider in that country and disregard all paths observed by monitors hosted in these potentially-biased AS_h. As in [31], we implement outlier filtering only where we have observations of $CTI_{m(AS_h)}(AS_t, C)$ from 10 or more AS_h, which occurs for 58.4% of transit AS-country pairs in our sample (a single AS can operate in multiple countries).

[9] Refer to [33] (§2.1.5 and §4.2.4) for an extended discussion of the intuition behind the CTI model.

5 Country-Level Transit

In this section we present the results of applying our CTI metric to the transit ecosystem of 75 countries with little-to-no international peering. (We describe our method for selecting these countries in §6.) We provide a high-level characterization of the transit ecosystem in each country by comparing the CTI scores of the top-5 ASes ranked by CTI (Sec. 5.1), as well as a set of ASes that appear in the top 5 of many countries (at least 10). Our hypothesis is that these countries show different transit profiles as a consequence of the socioeconomic and geopolitical diversity of the sample: from high exposure to observation, where one AS is the most influential transit provider and others are very marginal, to less exposed countries with an ensemble of ASes with similar values of CTI.

Investigating the companies operating the ASes with high CTI, we find two prominent groups of organizations: submarine cable operators (Sec. 5.2) and state-owned providers (Sec. 5.3). For the former, their operation of physical infrastructure connected to the country may underpin their high transit influence. With regards to state-owned ASes, providing transit may give governments the ability to expand their footprint beyond addresses they originate, *e.g.*, through a state-owned broadband provider. In some cases, state ownership of a transit provider may follow their investment in a submarine cable or landing station, while in others it may reflect the government's intention to enact censorship. We limit our analysis to the discovery of the transit footprint of the state, without delving into the underlying motives.

5.1 CTI distribution across countries

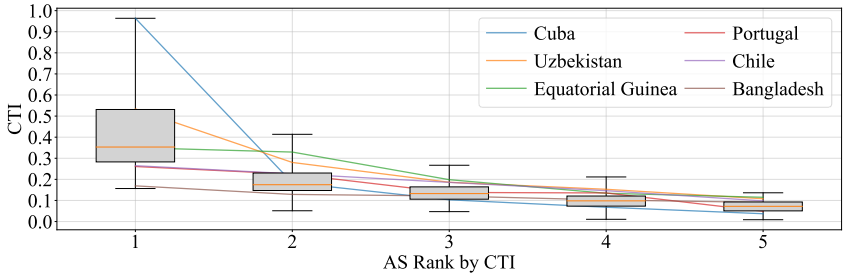


Fig. 3: Boxplot of CTI distributions for the top-5 ASes in each country.

In this subsection we present an overview of the CTI distribution across countries. Countries with a top-heavy distribution of CTI values are particularly exposed to specific networks. Other nations with a more flat distribution signal an ecosystem that is less exposed to prominent transit ASes. Fig. 3 shows the distribution of CTI values for ASes ranked in the top 5 by CTI in each country. In 51 countries, the top-ranked AS has CTI ≥ 0.3, signaling high exposure to observation and tampering by that specific network.

The distribution of CTI rapidly declines across AS rank, with the median halving from the first to the second position. In 54 countries, CTI declines by over 30% from the top-ranked AS to its successor; the average and median decline across all countries are 50% and 47%. This suggests that in the vast majority of countries in our sample, a single AS is particularly prominent in terms of its capabilities to observe or tamper with traffic.

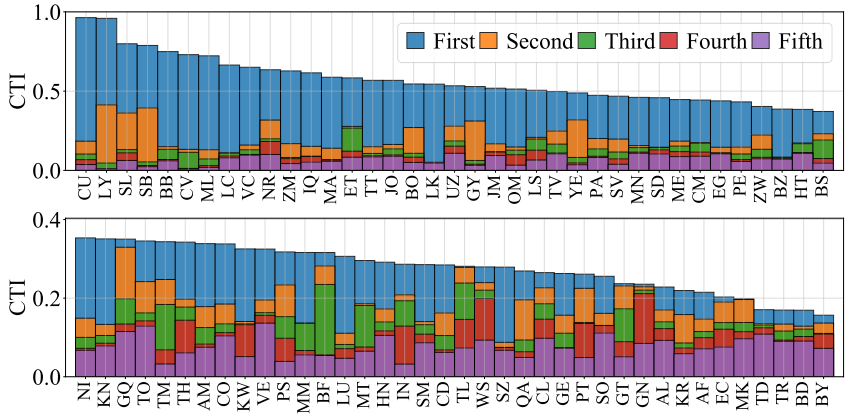


Fig. 4: Overlapping bars showing CTI values of the five top-ranked ASes in the 75 countries we study.

Individual nations. Results for the full set of countries we study[10] are included in Fig. 4. We discuss several representative cases below.

Most exposed countries. Only four countries have a top-ranked AS with a CTI over 0.75: Cuba, Libya, Sierra Leone, and the Solomon Islands (a small island nation). Cuba appears to have the most-exposed transit ecosystem[11], in which the top-ranked AS has CTI of 0.96. Because CTI discounts indirect transit—and the top AS monopolizes observed, direct connectivity—the CTI of Cuba's remaining ASes declines rapidly (81% from the top-ranked AS to the second).

Countries around the median. The median of the leftmost bar in Fig. 3 consists of countries that are still considerably exposed to observation and tampering, with CTI values ranging from 0.34 to 0.44, including: Egypt, Equatorial Guinea, Belize and Thailand. In Eq. Guinea, the top-two ASes each have a CTI over 0.3; these ASes have a p2c relationship with each other. Egypt and Belize

[10] Note that multiple ASes may provide transit connectivity to the same prefixes, explaining why the sum of CTI values of top ASes may be greater than 1.

[11] This is consistent with previous work that focused exclusively on Cuba, finding its international connectivity to be constrained [16].

have more skewed distributions, with a 67–79% decline from the top AS to its successor.

Least exposed countries. At the other end of the spectrum in Fig. 4 are five countries where the top-ranked has CTI values under 0.2: Chad, Bangladesh, Belarus, Turkey and North Macedonia. These countries have flatter distributions, with CTI declining at most 21% (or 16% on average) between the top-two ASes. As a result, we find no evidence of these nations being particularly exposed to a single network (unlike most of their peer countries in our sample). India, the country with the most Internet users in our sample, is in the bottom third with a top-AS CTI of 0.29, declining by 27% between the top-2 ASes.

Frequently top-ranked ASes. Of the 165 ASes present in Fig. 3, 126 of them are in the top-5 for only one country, with a further 31 ASes in the top-5 of at most 10 countries. There are eight notable exceptions, however: 3356*-Lumen[12] (top-5 in 25 countries), 1299*-Telia (24), 174*-Cogent (24), 6939-HE (18), 5511*-Orange (16), 6762*-T. Italia (14), 23520-C&W (14), and 6453*-Tata (12). Nearly all of these networks (marked with *) are in the inferred clique at the top of the global transit hierarchy [1]. C&W is only present in our analysis for countries in the Caribbean. HE has a very broad footprint, with countries in Africa (7), the Mid. East (3), W. Europe (2), Southeast Asia (2), South Pacific (2) and East/South Asia (1 each).

5.2 Submarine cable operators

Submarine cables are known to be an important part of the global Internet infrastructure [15,29,45] and play a role in the top-5 ASes of most countries we study. (Nicaragua, Guatemala, and Guyana are the only three nations where none of the top-5 ASes are associated with the submarine cables landing in the country.)

In this section, for each country, we find the highest-ranked AS by CTI where there is evidence of an institutional connection between the AS and an owner or operator of a submarine cable. We define an AS as a submarine cable operator if we find a direct match between the AS Name, the AS Organization [20], or a corporate parent organization (*e.g.,* CenturyLink for Level3, the Government of Sierra Leone for Sierra Leone Cable Company) and the owners of a submarine cable operator according to TeleGeography [64] and Infrapedia [38]. This process yields submarine cable ASes in 46 countries out of 51 possible, as 17 of the 75 countries are landlocked, and 7 have no submarine cable connectivity according to the operator databases. In three additional countries (Myanmar [4], the Solomon Islands [10], and Congo DRC [43]) only TeleGeography provides an AS to submarine cable match, which we confirm with information from the cited sources (the operators themselves, the government of Australia, and a submarine cable news source). In the remaining two countries (Thailand [65] and Samoa [63]) where we were not able to find an AS to submarine cable from TeleGeography, we rely on the cited sources (from the operator and a Samoan

[12] Formerly Level3/CenturyLink.

news outlet) to find a match. Note that only operators of submarine cables who appear as an AS on the BGP path can be identified using this method.

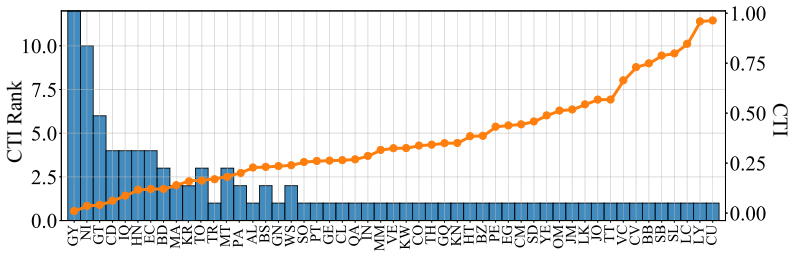


Fig. 5: Orange circles: CTI of top-ranked submarine cable AS. Blue bars: CTI rank of top-ranked submarine cable AS.

Our findings are shown in Fig. 5, with the CTI of the top cable-owning AS in each of the 51 countries shown as orange circles, and the ordinal ranking of that AS in its country's ecosystem as blue bars. In 36 countries, a submarine cable AS is ranked at the top by CTI, with an average rank of 1.9.

Note that being the top operator by CTI means different things in different countries, as the underlying potential exposure to observation affects the CTI of the top AS. For instance, in Turkey a cable-owning AS ranks first by CTI, but has the lowest CTI among such countries. Said AS (9121-Turk Telecom) has a CTI of 0.17. By contrast, in Cuba and Libya, a submarine cable operator (11960-ETECSA and 37558-LIT) is also ranked first but with CTIs of 0.96 in both cases. As a result, Turkey is much less exposed to a single AS than Cuba and Libya.

We also find regional clusters of high transit influence for the same AS operating a submarine cable, including C&W (formerly Columbus Networks), which is among the top providers in 11 countries in Central America and the Caribbean thanks to its ownership of the ECFS, ARCOS-1 and Fibralink cables. Telecom Italia Sparkle, Telefonica and Bharti Airtel also have an important transit presence in the Mediterranean, Latin America, and South Asia respectively. We release a complete list of submarine cables linked to an AS with high CTI on the paper's repository.

5.3 State-owned transit providers

In more than a third (26) of nations, we find that at least one of the top-5 ASes is state-owned, motivating us to further examine the total influence of a country's government on its Internet connectivity. In particular, we adapt CTI to quantify the influence of state-owned conglomerates—as some nations have

more than one state-owned AS—and apply it to the 75 countries in our sample. We use as input a list of ASes that are majority-owned by sovereign states [23]. The list was manually verified and encompasses both access and transit ASes. The dataset includes major telecommunication providers as well as its sibling networks and subsidiaries. Using this list, we find 100 state-owned ASes who operate domestically (*i.e.,* where the state owner and the country of operation are the same) in 41 countries.

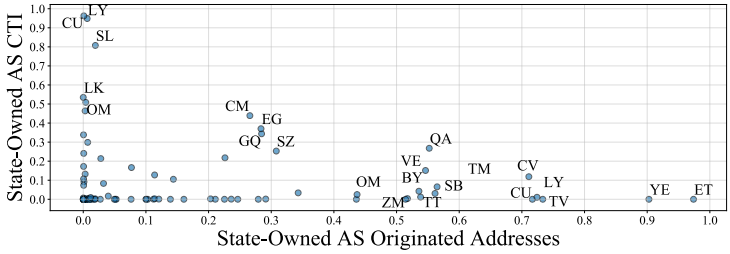


Fig. 6: CTI and fraction of addresses originated by domestic, state-owned ASes in our study.

Influence of state-owned ASes. Our initial exploration of the influence of state-owned ASes concerns the role each AS plays in the ecosystem of its country, as shown in Fig. 6. We find that state-owned ASes tend to provide either transit or access, usually not a combination of both. (Most points in Fig. 6 line up along an axis, rather than towards the middle.) As a consequence, meaningfully estimating the footprint of the state requires combining the two kinds of influence as well as aggregating data for AS conglomerates. (Two exceptions where a state-owned AS provides both Internet access (*i.e.,* as an origin AS) and serves transit to other ASes are Cameroon and Egypt; in the former, Camtel has both a high CTI (0.44, ranked first) and originates 27% of the country's addresses (second only to Orange Cameroon). Egypt's TE has a CTI of 0.37 and originates 28% of the country's addresses.)

We begin our combined estimation by computing CTI for not just a single AS, but a set of ASes, while not "double counting" influence over the same addresses; *i.e.,* if two of the state's ASes originate and provide transit to the same addresses, we add those addresses to the state's footprint once. We call this derived metric $CTIn$. Intuitively, $CTIn$ reflects the "pure-transit" footprint of the state, crediting only the addresses where state-owned ASes serve exclusively as transit providers. For instance, if AS A and AS B (both of which operate in country C) respectively originate and provide transit to the same /24 prefix, $CTIn$ says that the conglomerate $S_C = \{A, B\}$ does not have transit influence

over the /24 prefix. Formally, $CTIn_M(S_c, C) \in [0, 1]$ is calculated as

$$\sum_{m \in M} \left(\frac{w(m)}{|M|} \cdot \sum_{p | \text{onpath}^*(S_c, m, p)} \left(\frac{a(p, C)}{A(C)} \cdot \frac{1}{d^*(S_c, m, p)} \right) \right),$$

which is essentially identical to Eq. 1, except that S_c is a set containing all of the ASes in the state-owned conglomerate of country C; $\text{onpath}^*(S_c, m, p)$ is true if $\text{onpath}(AS_t, m, p)$ is true for some $AS_t \in S_c$ and p is *not* originated by any AS in S_c; and $d^*(S_c, m, p) = \min_{AS_t \in S_c} d(AS_t, m, p)$, *i.e.,* the AS-level distance from p to the closest AS in the conglomerate.

Finally, we define the total footprint of the state, *i.e.*, addresses that are either originated or for which transit is served by a state-owned AS. The state's footprint $F(C) \in [0, 1]$ is calculated as

$$F(C) = CTIn_M(S_c, C) + \sum_{AS_o \in S_c} \frac{a^*(AS_o, C)}{A(C)},$$

where $a^*(AS_o, C)/A(C)$ is the fraction of addresses in country C originated by AS_o. The first term of the sum is the pure-transit footprint and the second term is the addresses directly originated by the state-owned conglomerate S_c.

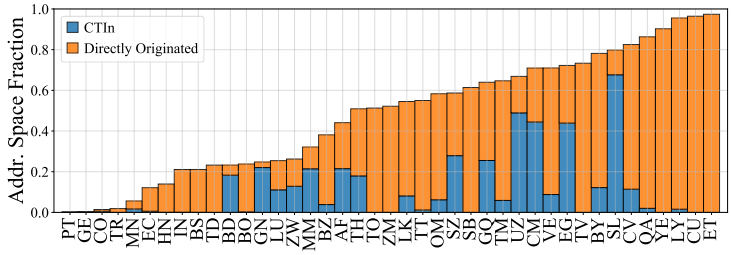


Fig. 7: State-owned originated address space a^* (orange bars), $CTIn$ (blue bars), and state footprint F (bar height) for countries in our study.

Findings. Fig. 7 shows our findings for the state-owned footprint (F, bar height), the originated fraction by state-owned ASes (orange bar), and pure-transit footprint of state-owned ASes ($CTIn$, blue bar). Our results suggest that domestic state influence exists on a spectrum where some countries, such as Ethiopia, Cuba, Libya and Yemen, rely overwhelmingly on the state for the provision of Internet access and (F between 0.90–0.97), whereas others, such as Colombia, Turkey, Mongolia and Ecuador have relatively marginal state-owned enterprises (F between 0.01–0.12).

Regarding the mode of influence that states use, in many countries in Fig. 7, most of the bar height is contributed by the orange portion, meaning that the footprint of the state comes from addresses directly originated. However, in some countries the state punches above its access network weight by deploying an influential transit provider, *i.e.,* those where the bar height is not dominated by the origin contribution in orange.

Table 1: Top countries by $CTIn$.

Country	SL	UZ	CM	EG	SZ	GQ	GN	AF	MM
$CTIn$	0.68	0.49	0.44	0.44	0.28	0.26	0.22	0.21	0.21
F	0.80	0.67	0.71	0.72	0.59	0.64	0.25	0.44	0.32

Pure-transit footprint of state-owned ASes. The countries where pure-transit influence ($CTIn$) is largest (0.2 or more, or pure-transit influence over at least a fifth of the country's addresses) are shown in Tab. 1. In these countries, all of which are in Africa and Central Asia, providing transit considerably increases the influence of the state. We note that the mere existence of these influential transit ASes does not signal willingness of the state to engage in surveillance or selective tampering, but rather that the government may have opportunities to do so. For instance, Myanmar's state-owned Myanma Posts and Telecommunications (MPT), which is included in our analysis, appears to have been involved in the disruption of the country's Internet service during the recent coup [36].

6 Inferring Transit Dominance

In this section, we describe how we identified the 75 countries that are the focus of the preceding section, *i.e.,* countries where provider-customer transit (p2c) relationships are likely the dominant mode of inbound international connectivity. We start by identifying countries for which public datasets of Internet Exchange Points (IXPs) and Private Colocation facilities (Colo) show no evidence of international peering (Sec. 6.1). Based on this analysis, we conduct an active measurement campaign to confirm the absence of international peering (Sec. 6.2). This second stage based on traceroutes is necessary because peering datasets are incomplete, particularly when it comes to membership lists at IXPs in developing countries [47]. We consider the prevalence of transit links being used to reach each of our target countries from probes distributed worldwide (§ 6.3) in combination with our operator validation (§7) to select a set of transit-dominant countries.

We define international peering as a (logical) link between two ASes that: *(i)* operate primarily in different countries (Sec. 3), and *(ii)* where that link is not an inferred transit-customer link. We use this definition since we are interested in studying the AS-level routes taken towards each country. We are aware of the limitations of our measurements and analysis, particularly with regards to the location (both topologically and geographically) of our probes; we address the issue further in Sec. 8.

6.1 Constructing a candidate list

We identify countries where international peering may not be prevalent by evaluating evidence of international peering involving origin ASes present in the

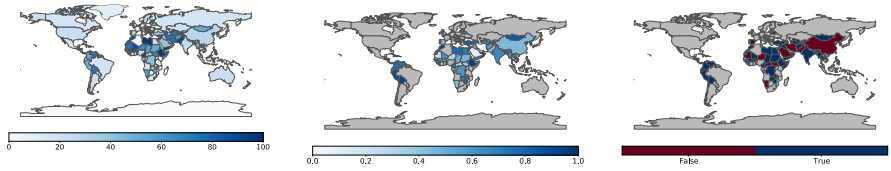
country. While domestic peering is very common, our hypothesis is that international peering is still not a frequent occurrence in some countries. We begin with the set of ASes that originate at least 0.05% of addresses in each country. We remove marginal ASes that originate a very small fraction of the country's address space to reduce the scope of our active campaign, as we are limited by RIPE Atlas's system-wide limits on concurrent measurements [55]. This set includes origin ASes that we classified as foreign to that country, but that originate BGP prefixes entirely geolocated in the country. (These ASes originate a marginal fraction of the addresses in the vast majority of countries we study; see §3). We look for these origin ASes in CAIDA's IXP dataset (from Oct. 2019 [21]), PeeringDB Colo dataset (from Mar. 1st, 2020 [9]), and inferred AS-Relationships from BGP (Mar. 2020 [5]).

We classify an origin AS as a *candidate* if the following three conditions are true:

1. the origin AS has no foreign peers in BGP [5];
2. the origin AS is not a member of any IXPs or Colos based in another country [21,9]; and
3. the origin AS is not a member of any IXPs or Colos where any member AS is based in a different country than the origin AS [21,9].

The intuition for each test is as follows. If we observe at least one foreign peer on BGP (1), this origin AS already has the ability to receive some external content from that peer, bypassing transit providers. Therefore, transit providers serving that origin will have fewer capabilities to observe traffic flowing towards it. Further, if an AS is a member of an IXP/Colo in another country (2), or a member of an IXP/Colo where another member is from a different country (3), the origin AS is at least capable of establishing peering relationships with those other ASes.

Fig. 8a shows the percentage of a country's address space originated by candidate ASes. We select the top-100 countries as candidates for active measurements. This set includes only countries where at least 25% of addresses are originated by candidate ASes. Our motivation is to actively probe the set of countries where it is most likely that transit providers still play an important role on inbound international connectivity. These 100 countries are colored in Fig. 8b.



(a) (b) (c)

Fig. 8: Non-peering observed perc. on passive datasets 8a, scaled country-level transit fraction in probed countries 8b, and final set, with countries in red excluded 8c.

6.2 Active measurement campaign

We ran a traceroute campaign to the 100 candidate countries for 14 days starting May 2nd, 2020. Additionally, we use all publicly available IPv4 traceroutes on RIPE Atlas during the same period—on the order of several million per hour—in order to opportunistically take advantage of other measurements towards the same ASes. We design our traceroute campaign guided by two constraints. First, we want to select a geographically and topologically diverse set of probes. Second, we have to operate within the rate limits of RIPE Atlas[13], particularly regarding concurrent measurements and credit expenditure.

Within these constraints, we launch ICMP traceroutes[14] from 100 active—shown as "connected" during the previous day [56]—RIPE Atlas probes (located outside any target country) towards a single destination in each AS, twice daily[15]; probing at this frequency gives us 28 opportunities to reach the AS during the two-week period from each vantage point.

We target an IP in a single /24 block for each origin AS in each candidate country by looking for any prefix originated by that AS that is entirely geolocated or delegated within the candidate country (see Sec. 3). Our final dataset is comprised of 33,045,982 traceroutes, including those launched by other RIPE users that meet our constraints. The distribution of the number of traceroutes reaching each country has the following properties: (Min, 25th Pctl., Median, Mean, 75th Pctl., Max) = (36, 13k, 46k, 330k, 250k, 3.3m). That is, the median country received 46k traceroutes. Only three countries received fewer than a thousand traceroutes: Eritrea (667), Nauru (154), and Tuvalu (36).

We use BdrmapIT [49] to translate our traceroutes into AS-level interconnections. BdrmapIT requires a number of external datasets in its operation, which we specify as follows: inferred AS-Level customer cone [48] from Mar. 2020; *AS2Org*, which infers groups of ASes who belong to the same organization[16], from Jan. 2020; and datasets we mention in other sections—prefix-to-Autonomous System mappings (§2), *PeeringDB* records (§6.1), and RIR delegation records (§3). From these traceroutes and external datasets, *BdrmapIT* infers a set of AS-level interconnections and the IP addresses (interfaces) at which they occur. Each interface inferred by *BdrmapIT* has an AS "owner" assignment. We reconstruct the AS-level path observed on the traceroute using such assignments.

6.3 Country-level transit fraction

From the preceding sections we have built a set of AS-level paths taken from the traceroute source to the destination AS. We now need a quantitative analysis technique to infer the prevalence of transit links on inbound traces towards each country.

[13] Which RIPE Atlas generously relaxed for this study upon direct request.
[14] Using default RIPE Atlas values except number of packets (reduced to 1).
[15] We space traceroutes an hour apart in 800-target IP blocks.
[16] This dataset is published quarterly.

To that end, we determine how frequently a transit (p2c) link is traversed when crossing the AS-level national boundary[17] towards an origin AS (AS_o) in a candidate country. We infer the AS-level national boundary as the link between the last foreign AS observed on the AS-level path (starting from the vantage point) and the subsequent AS.

We calculate how frequently, in the inbound traceroutes we process with *BdrmapIT*, the AS-level national border crossing occurs on a transit link for each origin AS. We scale this fraction to take into account the size of the address space originated by each AS using the *country-level transit fraction*:

$$T(C) = \sum_{AS_o, AS_c \in \mathrm{dom}(C)} \sum_{AS_t \notin \mathrm{dom(C)}} \frac{R(AS_o, AS_t, AS_c)}{R(AS_o)} \cdot \frac{a^*(AS_o, C)}{A(C)},$$

where $R(AS_o, AS_t, AS_c)$ is the number of traceroutes destined toward a prefix originated by AS_o that traverse a transit link between a foreign provider AS_t and a domestic customer AS_c in country C; $R(AS_o)$ is the total number of traceroutes where AS_o is the last observed AS; and $a^*(AS_o, C)/A(C)$ is the fraction of country C's address space originated by AS_o. For instance, if an AS originates 50% of the country's origin addresses, and 50% of the traces towards it traverse a foreign transit provider AS, the contribution of that AS to the country-level transit fraction becomes 0.25. Note that AS_c and AS_o are not necessarily the same, as the border crossing may occur at the link between (direct and/or indirect) providers of AS_o.

The values of $T(C)$ for each candidate country are represented in Fig. 8b: countries in darker shades of blue have both a large probed and responsive fraction and a large fraction of traceroutes from outside the country traversing transit providers. The closer the fraction is to 1, the more evidence we have that the country relies on transit providers for its international inbound connectivity.

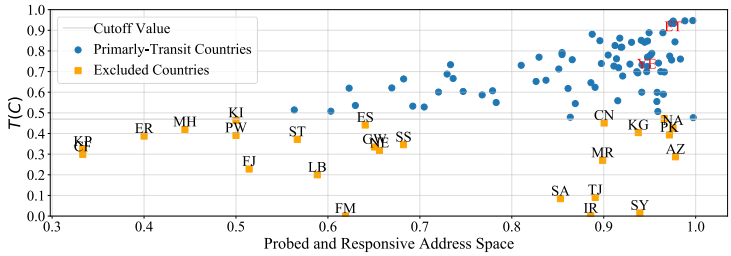


Fig. 9: Country-level transit fractions $T(C)$ for countries in our sample.

[17] As defined by our AS Nationality (§3), not actual political borders.

6.4 Final selection

Finally, in order to identify a set of primarily-transit countries, we evaluate the values of $T(C)$ across countries, shown in Fig. 9. At one extreme of Fig. 9 and Fig. 8b are countries such as Ethiopia (ET) and Yemen (YE), $T(C) = 0.95$ and 0.7, respectively, where all available evidence points towards transit links as the main inbound modality. At the other extreme are countries such as Syria (SY) and Iran (IR), $T(C) \leq 0.01$, where we rarely observe AS-level national borders being crossed using transit links.

Outside the upper and lower extremes in Fig. 9, where the decision of whether to include a country in our study is obvious, the middle results (most countries) do not offer clear dividing points. We decided then to set the threshold for $T(C)$ to classify a country as primarily-transit based on our validation with operators (§7); in particular, we use the value of $T(C)$ for Sudan (0.48) as a lower bound, which is the lowest $T(C)$ in any country that we were able to confirm relies on transit links for its inbound connectivity. The final countries in our CTI study are shown in a blue-white spectrum in Fig. 8c and as blue circles in Fig. 9, 75 of the 100 candidates. Countries in red are excluded from further analysis, as at this time we lack sufficient evidence to support that they are primarily using transit providers for inbound connectivity.

7 Stability and Validation

In this section, we discuss the findings of our stability analyses, validation with operators, and a calculation of transit influence at the organization level.

7.1 Stability

Temporal stability. We apply our CTI methodology to a set of BGP paths from Feb. 2020 and Apr. 2020 and compare the results to those presented in §5 (from Mar. 2020). Specifically, we compute the absolute value of the difference in CTI across successive months for transit ASes listed in each country. The results are shown in Tab. 2. We find that the CTI values are relatively stable across these months.

Table 2: CTI Temporal Stability Analyses.

Type	Compared Sets	25th ptile.	Mean	Median	75th ptile
Temporal	Feb. & Mar. 2020	0.00000	0.00190	0.00001	0.00016
All ASes	Mar. & Apr. 2020	0.00000	0.00156	0.00001	0.00017

Stability to changes in geolocation input. In order to assess the potential fragility of our study to inaccuracies in geolocation, we also applied our CTI methodology using MaxMind [3] and computed the absolute value of the difference in CTI scores produced with each location database. The output of this analysis is (25th perc.,mean,median,75th perc.) = 0.00000, 0.00104, 0.00002, 0.00017, suggesting CTI is relatively stable across these geolocation inputs.

7.2 Operator Validation

We discussed our findings with employees or contractors of two types of organizations: commercial network operators and non-profits who conduct networking research (universities, registrars, and non-commercial network operators). Additionally, we describe the results of our discussions follwing a mass email request to ASes with prefixes geolocated in countries in our study. Discussions with all of these organizations are anonymized. Our findings are largely consistent with each operator's view of the transit ecosystem of the countries discussed with them.

The results of our discussion of CTI findings with 6 operators in 6 countries[18] are shown in Tab. 3. Our CTI operator discussions consist of a confirmation of the AS set we identified as being most influential in their countries. Overall, operators confirm that the vast majority of ASes we identify are among the most influential in their nations. We also summarize our discussions with: *(i)* operators regarding our inferences of transit-dominant countries, *(ii)* ASes with prefixes geolocated to these countries. Regarding *(i)* 10 operators in 9 countries[19] confirmed that their nations are primarily transit[20].

Regarding *(ii)* we sent a mass email request to the WHOIS `abuse` address registered by ASes that had prefixes geolocated in 10 countries[21] (with IRB approval): BO, CO, VE, CM, BD, GT, CL, HN, SV and ZW[22]. We received 111 responses in 9 of these countries (all but ZW). Of these, 107 confirmed they operate primarily in the country that we geolocated their prefixes to[23]. Additionally, 108 were willing to discuss which type of business relationship dominated their inbound international traffic: 83 stated that transit relationships are the primary modality.

Table 3: CTI operator validation in 6 countries: CO, ET, ZW, SD, CD and CM.

AS-Country Pairs	#Confirmed	#Rejected	#Unconfirmed	Total #ASes
Top 5 ASes	27 (90%)	1 (3%)	2 (7%)	30
All Top ASes	45 (79%)	7 (12%)	5 (9%)	57

[18] We sent a set of ASes produced before updating our CTI methodology to its current form, which explains the "unconfirmed" column; the "top" ASes were defined as the country's top 12, unless any of those ASes had a marginal CTI score.

[19] CO, ET, CD, LS, SZ, ZW, VE, SD and CM.

[20] Sample, anonymized operator response: "Sudan is characterized by the traditional IP transit model. There is a domestic IXP, which serves five ISPs and [redacted AS Name]'s DNS nodes, but there are no foreign network operators present here. Furthermore, until recently, only two ISPs held gateway licenses (*i.e.,* were licensed to provide external connectivity to Sudan)."

[21] We only contacted ASes who had $\geq 1\%$ of their addresses in the country. Since this survey took place in 2021, we use the addresses geolocated in Jan. of that year.

[22] Selected as a mix of large & small (by #ASes) EN- and ES-speaking countries.

[23] In 3 cases, they stated that they operate in multiple countries.

7.3 Organization-Level Transit Influence

In some instances, multiple ASes may be operated by the same organization. We identified 323 instances where multiple ASes belonging the same organization (as of Jul. 2020 [20]) have $CTI > 0$ in a given country. We compute an upper bound of the organization's transit influence (in each country) by summing the CTI of component ASes. We find that 270 org-country pairs—an organization operating in a country—have marginal influence, with the CTI sum under 0.05 (218 were under 0.01).

For the remaining 53 organization-country pairs, we compute the contribution to the CTI sum of the highest-ranked AS in each organization. We separate these into three groups: *(i)* In 36 org-country pairs, the top AS contributes at least 90% of the CTI sum (98% on average). In these 36 cases, then, a single AS is responsible for the vast majority of the organization's transit influence. *(ii)* In 7 org-country pairs, the contribution to the CTI sum of the additional ASes—other than the top AS—in the organization is between 0.01–0.04 (between 11-29% of the CTI sum), or 0.02 on average. Therefore, the change in CTI as a result of their inclusion is relatively marginal.

(iii) In the remaining 10 org-country pairs, only 4 have a CTI sum greater than 0.1. For these, we compute the $CTIn$ of the organization to determine the contribution of the top AS in each organization (rather than a lower bound). In all 4 cases, the top AS contributes 61% or more of the organization's $CTIn$ (country-org, perc. of $CTIn$): VE-Lumen (87% of 0.16), SZ-Orange (61% of 0.14), WS-Lumen (73% of 0.30), and TV-Internap (62% of 0.11). Three of these countries are either a microstate (SZ) or a small island nation (WS and TV). The last instance, in Venezuela, is likely a consequence of the merger of two large companies: AS3356 (Level 3) and AS3549 (Global Crossing) [41].

8 Limitations

At a high level, CTI assumes all ASes and IP addresses are equivalent, which is certainly not the case. At the AS level, it is possible that one, dominant AS provides stronger security than a multitude of smaller ASes with tighter budgets. From the perspective of an attacker, though, a single AS having high CTI creates an opportunity; in the case of sophisticated attackers such as nation-states, the possibility of infiltration of any network cannot be discarded, but compromising many ASes simultaneously—in order to observe traffic towards countries where no AS has high CTI—may be more challenging. As such, ASes with very high CTI still present a concerningly large observation footprint, regardless of their level of security against infiltration[24].

Similarly, IP addresses can represent vastly different entities. Both access and transit ASes may deploy carrier-grade network access translation (CGNAT) [53]. Since our model treats all routed IPs equally, it does not currently take

[24] Recall that CTI studies exposure to *inbound* traffic observation or selective tampering, which is unaffected by potentially asymmetric AS paths.

into account the number of hosts multiplexing a single IP address. We leave this to future work, but note that an additional weight may be added to CTI: one that scales up the number of IP addresses in a given prefix by the number of hosts—or the number of "eyeballs"—connected to those IPs, on aggregate. Even within a given network, however, individual hosts are unlikely to be equally important as some (e.g., those belonging to governmental organizations or power-grid operators) may have more sensitive traffic. Conversely, some networks might not even actually use all their IP addresses—although the latter issue is likely less of a concern in the countries we have studied as their allocation of IPv4 addresses tends to be constrained [24].

In addition to this fundamental conceptual limitation, there are a variety of technical details that could have out-sized impact on our conclusions:

Incomplete BGP data. We acknowledge that the BGP paths we observe and use to compute CTI are incomplete given the location of BGP monitors. Given the serious implications for countries that appear highly exposed to external observation and selective tampering by an AS, we argue that it is important to study such exposure with available data. Further, we note that there are two important factors aiding the credibility of our CTI findings: *(i)* our validation with network operators, who have confirmed that the set of transit ASes identified in their countries is largely consistent with their own understanding of the country's routing ecosystem. *(ii)* There is greater visibility over p2c links in the AS-level topology [48,25], which enables our analysis as we are studying exposure to observation or selective tampering by transit ASes, in particular.

Despite these mitigating factors, we recognize that BGP incompleteness may impact the accuracy of CTI findings. We leave to future work an analysis of CTI's sensitivity to changes in the BGP input (which would further mitigate concerns with BGP incompleteness), *e.g.,* the addition or removal of BGP monitors, or the addition or removal of ASes who feed into each monitor. Finally, we note that CTI incorporates an outlier filter (§4.2 and §9.1) which has been shown as robust to changes in BGP input monitors [31].

Traffic. We use a country's geolocated IP(v4) addresses as a proxy for the nation's traffic, as this is a limited resource that is necessary to connect any device to the Internet. IP addresses are often used as a proxy for traffic, *e.g.,* in [61], and previous work has found strong correlations between number of IP addresses observed in BGP and traffic volume for ASes that provide either access or transit service [47]. An AS that serves a larger number of IP addresses would consequently have more capabilities for traffic observation, either of a larger share of potential devices, or of traffic that is more sensitive in nature.

Additionally, we do not study direct peering with cloud/content providers, who are responsible for large volumes of user-destined traffic. In addition to p2p links with access or transit networks, these content providers may have in-network caches in the countries we study. These caches may be placed in the access network itself, in the influential transit providers we have identified, or elsewhere [17]. Content providers are large and complex distributed systems, employing sophisticated load balancing [27], routing, and DNS [62] techniques.

Given these complexities, we leave to future work an evaluation of the impact on CTI of direct peering with cloud/content providers, and in-network cache placements.

Imperfect geolocation. A potential source of inaccuracy is IP geolocation, as assigning prefixes to a geographic area is challenging and the commercial providers who sell such information use proprietary methods. We have mitigated these concerns by calculating CTI using two commercial providers (§3), and find that the metric remains stable. We have also limited our analysis to the country level, where geolocation is more accurate than at finer granularities [18,52,35]. Further, while determining the location of prefixes originated by large transit providers with a global presence is problematic because of its dynamic nature and wide geographic spread, most networks are much smaller and will have limited geographic presence beyond their primary country of operation [69] (where most or all of their addresses will be located).

IPv6. Finally, we note that although our model has so far only been applied to IPv4 addresses—a reasonable scope given that IPv6 deployment is far from wide in many developing regions, including Africa [13,46]—the code libraries and software tools we have used are compatible with IPv6, enabling future research in this area.

Inferring Primarily-Transit Countries. Any active campaign launched using publicly available infrastructure will be limited in its effectiveness to reveal peering links by the location of vantage points (VPs) from which the traceroutes are launched. Our campaign is no exception: our VPs are located in a small subset of the world's ASes, and primarily in Europe and North America. However, we argue that our measurements form a sufficient basis to infer that, in the countries we have identified, foreign peering is rare, since: *(i)* we discussed our findings with operators in 12% of these countries, all of whom have confirmed that their nation relies primarily on transit providers to receive traffic from other countries since foreign peering there is rare to nonexistent; *(ii)* while our measurements are launched primarily from the U.S. and Europe, these regions do serve as important content sources and transit hubs (incl. for intracontinental traffic) for countries in Latin America, the Caribbean and Africa [16,32,40,34,30], where most of the nations we have identified are located.

9 Related Work

Several previous studies have focused on country-level routing, both for the identification of topological bottlenecks [58,42] and to evaluate the impact of specific countries' ASes on routes towards other countries [39]. All of these studies have used delegation data to map an entire AS to a country; these inferences are prone to inaccuracies when compared with more accurate and granular data such as IP-level geolocation, as important transit ASes may span multiple or many countries, or operate in a country different from their registration.

Previous work focused on the topologies of specific countries (Germany [66] and China [68]) and relied on country-specific methods and data sets that do not

generalize to automatic inference of AS influence in any given country. Fanou *et al.* [28] studied the interdomain connectivity of intracontinental paths in Africa, using a large traceroute campaign (rather than BGP paths).

CAIDA's AS Rank [48] is another topological metric developed to characterize the customer footprint of an AS on the global routing system. It does not try to capture the capabilities for observation of a transit AS for traffic flowing towards a country; we developed the CTI metric to try to do so.

9.1 National Chokepoint Potential and Hegemony

In this subsection, we describe differences between CTI and two closely related metrics, *National Chokepoint Potential (NCP)* [42] and *Hegemony* [31].

NCP. Leyba *et al.* [42] identified topological bottlenecks, a framework that would also help in quantifying exposure to observation (as CTI aims to address), but with some methodological differences, including: they identify transnational links towards each country using delegation records, and they define bottleneck ASes as those serving the most paths (rather than IP addresses). Further, both CTI and Leyba *et al.* [42] have as a goal the identification of international inbound—and, in their case, also outbound—*chokepoints* (*i.e.,* topological bottlenecks) in each country, based on actual (CTI) or simulated (NCP) BGP paths towards each origin AS. However, their work does not try to capture the fraction of the country's addresses served by a transit provider, but rather the fraction of paths that a border AS (*i.e.,* an AS which is registered to the same country as the origin, but which has a neighbor that is registered to another country) may be able to intercept. Our work is more narrowly focused on the specific case of a transit provider serving traffic towards a transit-dominant country, taking into account the address space of the direct or indirect customers. Conceptually, weighting by paths enhances the influence—or potential, in Leyba *et al.*'s terminology—of ASes frequently serving a broad share of the country's networks, whereas weighting by IPs yields higher influence to ASes frequently serving a large fraction of the country's end hosts.

Hegemony. Our country-level transit influence metric is perhaps most similar to Hegemony [31]. Both metrics aim to identify the transit ASes that are most prevalent on paths towards origin ASes, weighted by the IP address space they serve. Hegemony can be applied either to the global AS-level graph, or to a "Local graph: ... made only from AS paths with the same origin AS" [31]. The latter application is closest to CTI, as this analysis is limited to paths reaching a single origin AS; indeed, we use some of Hegemony local's filtering techniques in our analysis (Sec. 4.2). The applicability of (local-graph) Hegemony to the problem of revealing which transit ASes have observation capabilities over traffic flowing towards a specific country—the issue addressed by CTI—is limited, as Hegemony is a metric of centrality of transit ASes on a specific origin AS (not a country).

We build a country-level alternative metric based on Hegemony [31] and compare CTI to it. The reason for the comparison is to determine if CTI is too aggressive in its filters, discarding too much input data. For that purpose,

we build a benchmark using Hegemony local, a metric of centrality of any AS (including both transit providers and peers) on paths towards a single origin. Hegemony consists mostly of a single filter on input BGP data, making it an appropriate benchmark. This benchmark was not trivial to build, as Hegemony local produces a bilateral metric of influence between a transit AS and an origin AS on the global topology. While Hegemony is concerned with extracting the most accurate estimate of centrality on an existing graph, and not with estimating country-level inbound route diversity as CTI, it is possible to build a metric that serves a similar purpose as CTI, which we call *country-level Hegemony* (CLH) as

$$CLH(AS_t, C) \in [0,1] = \sum_{AS_o \in (C)} H(AS_t, AS_o) \cdot \frac{a^*(AS_o, C)}{A(C)},$$

where $H(AS_t, AS_o)$ is the Hegemony score of AS_t on AS_o during the same period[25] in March 2020 when we applied CTI, (all the other terms have been previously introduced in Eq. 6.3).

We computed the absolute value of the difference between CTI and CLH for each AS-coutry pair. The output of this analysis is (25th perc.,mean,median,75th perc.) = 0.00000, 0.00104, 0.00002, 0.00017, suggesting that both metrics tend to agree about the country-level influence of marginal ASes (the vast majority of AS-country pairs). Therefore, we find no evidence that the heuristics of CTI introduce unnecessary noise to our analysis because, on aggregate, a country-level alternative based on Hegemony—which excludes considerably fewer BGP monitors than CTI does—tends to agree with CTI's assessment. The metrics do diverge on their assessment of ASes that CTI has identified as influential (CTI$\geq$0.1), with an avg. difference between the metrics in those cases of 0.07.

10 Conclusions and Future Work

In this work we tackled the issue of quantifying the exposure of a country's traffic to observation or tampering by specific ASes. The Country-Level Transit Influence (CTI) metric we developed aims to overcome several challenges with making such inferences using BGP data. We apply this metric in a set of—potentially at-risk—countries where transit provider-customer relationships are still the dominant inbound modality for international traffic; we identified these nations using both passive and active measurements. We applied CTI in these 75 countries and found that the median nation has 35% of their IP addresses served by a single transit AS.

In the future, we would like to develop measurement and analysis techniques that can be applied to study the exposure of countries that are not primarily served by transit providers, but rather by a dense mesh of bilateral and multilateral peering agreements, including those involving cloud providers and CDNs.

[25] As Hegemony is published in 15-min intervals [11], we take the 5-day average score.

Acknowledgements

We thank our shepherd Amreesh Phokeer and the anonymous reviewers for their insightful comments, and Amogh Dhamdhere and kc claffy for providing generous feedback. We are grateful to the network operators who enabled our validation efforts. This work was partly funded by the National Science Foundation (NSF), Grant No. CNS 1705024. Author Gamero-Garrido was supported in part by the Microsoft Research Dissertation Grant (2019) and Northeastern University's Future Faculty Fellowship (2021).

References

1. As rank : About. https://asrank.caida.org/about. (Accessed in May 2021).
2. Internet users - the world factbook. https://www.cia.gov/the-world-factbook/field/internet-users/country-comparison. (Accessed in May 2021).
3. Maxmind geolocation data. https://www.maxmind.com/en/geoip2-services-and-databases.
4. MPT, China Unicom Plan International Cable to Boost Internet Connectivity. https://www.submarinenetworks.com/news/mpt-china-unicom-plan-international-cable-to-boost-internet-connectivity, 2013.
5. CAIDA AS-Relationships. http://data.caida.org/datasets/as-relationships/, 2019.
6. RIPE Routing Information Service (RIS). https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris, 2019.
7. RIR Delegation Files. https://ftp.ripe.net/pub/stats/ripencc/, 2019.
8. RouteViews. http://www.routeviews.org/routeviews/, 2019.
9. CAIDA's PeeringDB dumps. data.caida.org/datasets/peeringdb/, 2020.
10. Coral Sea Cable System. www.coralseacablesystem.com.au/about/, 2020.
11. Hegemony API. https://ihr.iijlab.net/ihr/api/hegemony/, 2020.
12. Netacuity. http://info.digitalelement.com/, 2020.
13. E. Agbaraji, F. Opara, and M. Aririguzo. Ipv6 deployment status, the situation in africa and way out. *IJAET*, 2(1):315, 2012.
14. A. Akella, S. Seshan, and A. Shaikh. An empirical evaluation of wide-area internet bottlenecks. In *IMC*, pages 101–114, 2003.
15. Z. S. Bischof, R. Fontugne, and F. E. Bustamante. Untangling the world-wide mesh of undersea cables. In *HotNets '18*, page 7884, NY, USA, 2018. ACM.
16. Z. S. Bischof, J. P. Rula, and F. E. Bustamante. In and out of cuba: Characterizing cuba's connectivity. In *IMC '15*, pages 487–493, New York, NY, USA, 2015. ACM.
17. T. Böttger, F. Cuadrado, G. Tyson, I. Castro, and S. Uhlig. Open connect everywhere: A glimpse at the internet ecosystem through the lens of the netflix cdn. *SIGCOMM Comput. Commun. Rev.*, 48(1):2834, Apr. 2018.
18. Bradley Huffaker and Marina Fomenkov and kc claffy. Geocompare: a comparison of public and commercial geolocation databases. CAIDA Tech Report, 2011.
19. X. Cai, M. Rey, C. xuecai, J. Heidemann, C. johnh, and W. W. Niksun. A holistic framework for bridging physical threats to user qoe usc / isi technical report. 2013.
20. CAIDA. AS2Org. https://www.caida.org/research/topology/as2org/, 2020.
21. CAIDA. CAIDA IXP Dataset. https://www.caida.org/data/ixps/, 2020.
22. CAIDA. Routeviews Prefix-to-AS mappings (pfx2as) for IPv4 and IPv6. http://data.caida.org/datasets/routing/routeviews-prefix2as/, 2020.

23. E. Carisimo, A. Gamero-Garrido, A. C. Snoeren, and A. Dainotti. Identifying ases of state-owned internet operators. In *IMC '21*, NY, USA, 2021. ACM.
24. Dainotti, A. and Benson, K. and King, A. and claffy, k. and Glatz, E. and Dimitropoulos, X. and Richter, P. and Finamore, A. and Snoeren, A. Lost in Space: Improving Inference of IPv4 Address Space Utilization, Oct 2014.
25. A. Dhamdhere and C. Dovrolis. Ten Years in the Evoultion of the Internet Ecosystem. In *ACM Internet Measurement Conference (IMC)*, 2008.
26. A. Edmundson, R. Ensafi, N. Feamster, and J. Rexford. Nation-state hegemony in internet routing. In *COMPASS '18*, NY, USA, 2018. ACM.
27. X. Fan, E. Katz-Bassett, and J. Heidemann. Assessing affinity between users and cdn sites. In *TMA*, pages 95–110, Cham, 2015. Springer.
28. R. Fanou, P. Francois, and E. Aben. On The Diversity of Interdomain Routing in Africa. In *PAM*, 2015.
29. R. Fanou, B. Huffaker, R. Mok, and k. claffy. Unintended consequences: Effects of submarine cable deployment on Internet routing. In *PAM*, Mar 2020.
30. R. Fanou, F. Valera, P. Francois, and A. Dhamdhere. Reshaping the african internet: From scattered islands to a connected continent. *Comput. Commun.*, 113:25 – 42, 2017.
31. Fontugne, Romain and Shah, Anant and Aben, Emile. The (thin) Bridges of AS Connectivity: Measuring Dependency using AS Hegemony. In *PAM*, 2018.
32. H. Galperin. Connectivity in latin america and the caribbean: The role of internet exchange points. 2013.
33. A. Gamero-Garrido. *Transit Influence of Autonomous Systems: Country-Specific Exposure of Internet Traffic*. PhD thesis, UC San Diego, 2021.
34. G. Garcia. Why miami is latin america's center of interconnection - interconnections - the equinix blog. `https://blog.equinix.com/blog/2018/05/01/why-miami-is-latin-americas-center-of-interconnection/`, May 2018.
35. Gharaibeh, Manaf and Shah, Anant and Huffaker, Bradley and Zhang, Han and Ensafi, Roya and Papadopoulos, Christos. A look at router geolocation in public and commercial databases. In *IMC*, 2017.
36. C. Giles. Myanmar coup: How the military disrupted the internet - bbc news. `https://www.bbc.com/news/world-asia-55889565`. (Accessed on 02/05/2021).
37. A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett. Peering at the internet's frontier: A first look at isp interconnectivity in africa. In M. Faloutsos and A. Kuzmanovic, editors, *PAM*, 2014.
38. Infrapedia. Infrapedia. `https://www.infrapedia.com/app`, 2020.
39. J. Karlin, S. Forrest, and J. Rexford. Nation-State Routing: Censorship, Wiretapping, and BGP. In *CoRR*, 2009. `http://arxiv.org/abs/cs/0608082`, 2009.
40. D. Kiedanski and E. Grampn. Understanding latin america ipv6 connectivity: A preliminary exploration. In *SCCC*, pages 1–6, 2017.
41. Level 3 Completes Acquisition of Global Crossing. `https://www.lightreading.com/ethernet-ip/ethernet-services/level-3-completes-acquisition-of-global-crossing/d/d-id/690402?`, 2011.
42. K. G. Leyba, B. Edwards, C. Freeman, J. R. Crandall, and S. Forrest. Borders and Gateways: Measuring and Analyzing National AS Chokepoints. In *COMPASS*, 2019.
43. Liquid Telecom. Network. `https://www.liquidtelecom.com/about-us/our_network`, 2020.
44. J. Liu, W. Peng, Y. Yang, and Z. Huang. A delay-based analysis of multiple bottleneck links of end-to-end paths in the internet. In Z. Sun and Z. Deng, editors, *CIAC '13*, pages 93–103. Springer, 2013.

45. S. Liu, Z. S. Bischof, I. Madan, P. K. Chan, and F. E. Bustamante. Out of sight, not out of mind: A user-view on the criticality of the submarine cable network. In *IMC '20*, pages 194–200, NY, USA, 2020. ACM.
46. I. Livadariu, A. Elmokashfi, and A. Dhamdhere. Measuring ipv6 adoption in africa. In *e-Infrastructure and e-Services for Developing Countries*, Cham, 2018.
47. A. Lodhi, N. Larson, A. Dhamdhere, C. Dovrolis, and k. claffy. Using PeeringDB to Understand the Peering Ecosystem. In *ACM CCR*, 2014.
48. M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and K. Claffy. AS relationships, customer cones, and validation. In *ACM IMC*, 2013.
49. A. Marder, M. Luckie, A. Dhamdhere, B. Huffaker, J. Smith, and k. claffy. Pushing the Boundaries with bdrmapIT: Mapping Router Ownership at Internet Scale. In *Internet Measurement Conference (IMC)*, pages 56–69, Nov 2018.
50. A. Mauldin. Is your planned submarine cable doomed? `https://blog.telegeography.com/is-your-planned-submarine-cable-doomed`, 2019.
51. B. Mbaye, A. Gueye, D. Banse, and A. Diop. Africa's online access: What data is getting accessed and where it is hosted? In *Innovations and Interdisciplinary Solutions for Underserved Areas*, pages 50–61, Cham, 2019. Springer.
52. I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye. Ip geolocation databases: Unreliable? *SIGCOMM CCR*, 41(2):53–56, Apr. 2011.
53. P. Richter, F. Wohlfart, N. Vallina-Rodriguez, M. Allman, R. Bush, A. Feldmann, C. Kreibich, N. Weaver, and V. Paxson. A multi-perspective analysis of carrier-grade nat deployment. In *IMC '16*, pages 215—229, NY, USA, 2016. ACM.
54. RIPE NCC. Probes. `https://atlas.ripe.net/probes/`, 2020.
55. RIPE NCC. RIPE Atlas - User-Defined Measurements. `https://atlas.ripe.net/docs/udm/`, 2020.
56. RIPE NCC. RIPE Atlas Probe Archive. `https://ftp.ripe.net/ripe/atlas/probes/archive/`, 2020.
57. RIPE NCC. RIS - RIPE Network Coordination Center. `http://www.ris.ripe.net/peerlist/all.shtml`, 2020.
58. Roberts, Hal and Larochelle, David and Faris, Rob and Palfrey, John. Mapping Local Internet Control. Tech Report, Berkman Center, Harvard University, 2011.
59. RouteViews. Collectors - RouteViews. `http://www.routeviews.org/routeviews/index.php/collectors/`, 2020.
60. A. Shah, R. Fontugne, and C. Papadopoulos. Towards characterizing international routing detours. In *AINTEC '16*, page 1724, New York, NY, USA, 2016. ACM.
61. F. Soldo and A. Metwally. Traffic anomaly detection based on the ip size distribution. In *2012 Proceedings IEEE INFOCOM*, pages 2005–2013, 2012.
62. A.-J. Su, D. R. Choffnes, A. Kuzmanovic, and F. E. Bustamante. Drafting behind akamai (travelocity-based detouring). In *ACM CCR*, NY, USA, 2006. ACM.
63. Talanei. ASH Cable buys bandwidth from Tui Samoa. `https://www.talanei.com/2018/05/10/ash-cable-buys-bandwidth-from-tui-samoa/`, 2020.
64. TeleGeography. Submarine Cable Map. `www.submarinecablemap.com`, 2020.
65. TOT Public Company Limited. TOT: INTERNATIONAL SUBMARINE CABLE. `https://www.boi.go.th/upload/content/tot_5d254fe992f21.pdf`, 2020.
66. Wahlisch, Matthias and Schmidt, Thomas and de Brun, Markus and Haberlen, Thomas. Exposing a Nation-Centric View on the German Internet - A Change in Perspective on AS-level. In *PAM*, 2012.
67. A. Zeitoun, Chen-Nee Chuah, S. Bhattacharyya, and C. Diot. An as-level study of internet path delay characteristics. In *IEEE Global Telecommunications Conference, 2004. GLOBECOM '04.*, volume 3, pages 1480–1484 Vol.3, 2004.

68. S. Zhou, G. Zhang, and G. Zhang. Chinese Internet AS-Level Topology. *IET Communications*, 2(1), Apr. 2007.
69. R. Zhuo, B. Huffaker, k. claffy, and S. Greenstein. The impact of the general data protection regulation on internet interconnection. *Telecomm Policy*, 45 (2), 2021.

A BGP Monitor Location and CTI Process Diagram

A.1 BGP Monitor Location

We begin with the 685 monitors in RIPE and RouteViews. We discard (91) monitors aggregated at multi-hop collectors and monitors that are not full-feed, so we are left with 350 monitors in 209 ASes. We determine the location of each full-feed BGP monitor as follows. First, we find the locations of RouteViews and RIPE RIS BGP collectors. We build a first set of locations by finding RIPE Atlas probes co-located at Internet Exchange Points (IXPs), by searching the list of peers for the IXP name, and assign that probe to the country where the (single-location) IXP is present, *e.g.,* BGP RRC01 – LINX / LONAP, London, United Kingdom. We confirm the BGP monitor location by running `ping` measurements from RIPE Atlas probes hosted at the IXP to the BGP monitor's IP address, and conclude that the BGP monitor is in the same city as the IXP if the RTT is lower than 5 ms. For the remaining BGP monitors we look for available RIPE Atlas probes in the ASes that peer with the same BGP collector, and similarly run `ping` measurements towards both the BGP monitor's IP address and a RIPE Atlas probe located in the same city as the one listed for the monitor. We conclude that the BGP monitor and RIPE Atlas probe are in the same city if both sets of RTTs are under 5 ms.

We exclude 118 monitors at this stage because there is no available RIPE Atlas probe hosted at the IXP (in the city where the monitor is listed) nor at any of the other peers of the collector aggregating announcements from the BGP monitor. We discard remote peers from our set, those that have `ping` RTTs higher than 30 ms from the RIPE Atlas probe in the BGP monitor's listed city. For monitors with an RTT between 5–30 ms, we infer them to be at the listed location if we get confirmation using DNS records—*i.e.,* we find a geographical hint such as a three-letter city or airport code, or the full name of the city, using a reverse lookup with the BGP monitor's IP address—or a matching country of the BGP monitor's `peer_asn` record in the RIPE RIS or RouteViews collector list [59,57]. Our final set M has 214 monitors in 145 ASes and 19 countries. We quantify the aggregate impact of all of our filters, including the exclusion of certain BGP monitors per country, in §9.1, given an alternative metric built using previous research [31].

A.2 CTI Process Diagram

We show a process diagram of our methodology in Fig. 10. There, our transit-dominance country selection is shown in the top right corner, while the remaining blocks on the top row refer to CTI inputs and preprocessing steps. Finally, the bottom row shows the core components of the CTI metric.

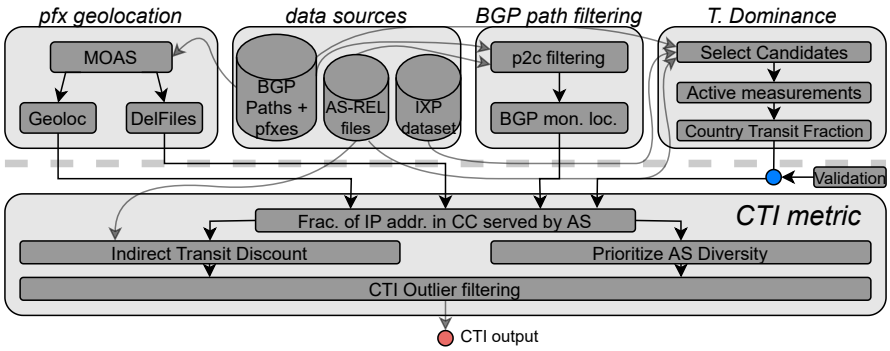


Fig. 10: Process diagram showing input sources and analyses that produce our model of AS-level connectivity, the CTI metric.

Jitterbug: A new framework for jitter-based congestion inference

Esteban Carisimo[1], Ricky K. P. Mok[2], David D. Clark[3], and kc claffy[2]

[1] Northwestern University {esteban.carisimo}@northwestern.edu
[2] CAIDA, UC San Diego {cskpmok, kc}@caida.org
[3] MIT {ddc}@csail.mit.edu

Abstract. We investigate a novel approach to the use of jitter to infer network congestion using data collected by probes in access networks. We discovered a set of features in jitter and *jitter dispersion* —a jitter-derived time series we define in this paper— time series that are characteristic of periods of congestion. We leverage these concepts to create a jitter-based congestion inference framework that we call *Jitterbug*. We apply Jitterbug's capabilities to a wide range of traffic scenarios and discover that Jitterbug can correctly identify both recurrent and one-off congestion events. We validate Jitterbug inferences against state-of-the-art autocorrelation-based inferences of recurrent congestion. We find that the two approaches have strong congruity in their inferences, but Jitterbug holds promise for detecting one-off as well as recurrent congestion. We identify several future directions for this research including leveraging ML/AI techniques to optimize performance and accuracy of this approach in operational settings.

1 Introduction

The general notion of network congestion – demand exceeds capacity for network (link capacity or router buffer) resources – is widespread on the Internet, and an inherent property of traditional TCP dynamics. A TCP connection endpoint induces congestion to infer its appropriate sending rate, increasing this rate until it fails to receive acknowledgement of receipt of a packet by the other endpoint, i.e., infers congestion based on packet loss [19]. More recent attempts to improve TCP's congestion control algorithms rely on increased latency rather than packet loss as a signal of congestion [22,7,8,35].

Outside of protocol dynamics, latency and loss are still the fundamental metrics used to detect episodes of network congestion, or more generally path anomalies that degrade performance [13,14,30,17,12,15]. Although researchers have developed autocorrelation techniques to infer persistent recurrent patterns congestion [12], the challenge of detecting one-off episodes of congestion in traffic data remains an open problem after 30 years of Internet evolution. One-off episodes of congestion have many causes, including traffic management transitions, router operating system overheads, network configuration errors, flash crowds (e.g., software releases), and DDoS attacks. Inferring congestion from

these phenomenological events is still an open challenge for the research network community.

We propose a new framework – Jitterbug – to use jitter and other metrics derived from round-trip-time (RTT) measurements to infer congestion. RTT measurements alone are often insufficient to infer congestion episodes, but we found that jitter-related metrics can distinguish congestion from other path anomalies, e.g., route changes. Specifically, we identify a correlation between periods of elevated latency (minimum RTT) and changes in the profile of jitter signatures – *jitter dispersion* – during congestion episodes. Relying on this concept, we develop a new framework that allows us to extend interdomain congestion inferences from recurrent patterns to one-off congestion events, i.e., discern recurrent from one-time congestion events. Using data collected between 2017 and 2020, this novel approach obtains similar results to state-of-the-art autocorrelation-based methods [12], but overcomes the limitation of the autocorrelation methods that can only detect recurrent periodic patterns of congestion. We find that Jitterbug introduces a promising approach to detect one-off congestion events. Our contributions are:

1. We identified a set of features in jitter and jitter dispersion time series, including a change of regime or transitory increase of the jitter dispersion, that characterize periods of congestion.
2. We used these features to develop and implement Jitterbug, a new jitter-based congestion inference method that combines pre-existing approaches to change point detection with information embedded in jitter signals.
3. We applied the Jitterbug framework to a wide range of challenging traffic scenarios, and explain its inferences.
4. We compare Jitterbug congestion inferences to the state-of-the-art autocorrelation-based methods [12], finding strong consistency in autocorrelation-applicable scenarios, i.e., for recurrent periodic congestion.
5. We release the source of code of Jitterbug[4].

The rest of the paper is structured as follows. We provide context by describing the latency model (§2.1) and jitter signatures in multiple real-world examples (§2.2). Leveraging these concepts, §3 describes Jitterbug and its components in detail. §4 describes the dataset we use to *(i)* investigate Jitterbug congestion inferences in different scenarios (§5), and *(ii)* cross-validate Jitterbug congestion inferences against other methods (§6). §7 summarizes lessons we learned during our study. §8 provides an extensive list of related work and §9 discusses open challenges in congestion inference. Finally, §10 offers concluding thoughts.

2 Background on RTT and Jitter Signatures

To provide context, we describe the latency model (§2.1) and four typical signatures we extract from RTTs and jitter (§2.2).

[4] Jitterbug repository: https://github.com/estcarisimo/jitterbug

2.1 Latency model

Round-trip time (RTT) in end-to-end measurements comprises both deterministic and random components. Eqn. (1) depicts the components of RTT between source (u) and destination (v) for a packet traversing a total of H hops in the round-trip path [21].

$$RTT(u,v) = d_{icmp} + \sum_{i=0}^{H}(d_s(i) + d_{prop}(i) + d_q(i) + d_{proc}(i)), \tag{1}$$

where d_{icmp} is the processing delay of ICMP messages in routers. d_s, d_{prop}, and d_{proc} represent delay induced by serialization, propagation, and packet processing, respectively. These deterministic components do not depend on traffic volume or link utilization. In contrast, d_{icmp} and d_q are random variables and contribute RTT variance, because their values depend on router CPU utilization and queue size of network interfaces when packets arrive. Prior work [23,12] has shown that RTT correlates with bottleneck link utilization, indicating that the queuing delay is the dominant factor in delay variation. Delay jitter, also referred to as jitter or IP packet delay variation [10], is the absolute difference between the current RTT value and the reference value of the previous time episode (i.e., $J_T = RTT(u,v)_T - RTT(u,v)_{T-1}$), where T is the current time episode. In this work we develop and evaluate a framework for using simple RTT and jitter-based metrics to classify path anomalies.

2.2 Analyzing RTT and jitter signatures in congested links

We use four real-world examples to illustrate the challenges and opportunities of using RTT and jitter to detect and identify path anomalies (Fig. 1). We focus on three properties of RTT and jitter to characterize the nature of path anomalies: *periodicity, amplitude, variability.*

Periodicity captures events that recur at a fixed frequency and duration, such as diurnal variations.

Amplitude measures the degree of changes in RTTs from the baseline. During network congestion events, probe packets are more likely to experience queuing delay. The elevation of RTTs reflects the queue size in the bottleneck link.

Variability refers to the stability of RTTs during the elevated periods, which allows us to discern congestion from other path anomalies such as a route change.

Fig. 1 shows four examples of two-week RTT and jitter time series measured from four vantage points in the U.S. to four router interfaces on the far-side[5] of interdomain links. Two examples (Fig. 1a and 1b) show periodic inflation in RTTs (blue/orange curves), indicating recurring congestion events. However,

[5] We referred as *near* and *far* sides to consecutive IP pairs in a traceroute path following the convention defined by Luckie *et al.* [23].

the jitter amplitude (green curve) in Fig. 1b, is much lower than that of Fig. 1a, consistent with a smaller queue size in the bottleneck link. Previous use of autocorrelation methods have shown that such persistent diurnal elevations in RTT at the far-side of an interdomain are evidence of interdomain congestion [12]. In contrast, the two cases in Fig. 1c and 1d are one-off events. The interesting difference is that in Fig. 1d the jitter increases as the RTT baseline jumps from 20ms to 40ms. In contrast, in Fig. 1c the jitter remains stable throughout. We suspect that this latter scenario was a route change event rather than congestion.

Although many different approaches to RTT change point detection could partition these time series into intervals, an approach solely based on RTTs would fail to distinguish congestion from other path anomalies such as route changes. The RTT signal is simply too noisy. This example shows that evaluating changes in jitter can enable us to differentiate these scenarios and thus we should consider jitter as a metric for characterizing path anomalies.

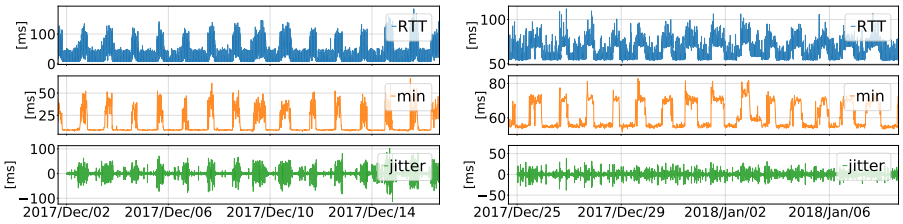
We next introduce our framework to support systematic analysis and classification of type of path anomalies with three properties that we extract from RTT and jitter time series data.

3 Jitterbug: Jitter-based congestion inference

Fig. 2 shows the building blocks of our framework, which combines change point detection algorithms (§3.2) with simultaneous analysis of minimum RTT and jitter time series obtained from latency measurements. The change point detection algorithm splits RTT timeseries into *candidate* time intervals that might suffer from congestion. The next step of the framework is to analyze the jitter in each time interval to classify candidate intervals as congestion events or other path anomalies. We infer congestion based on the three elements we observed in §2.2: changes in baseline RTT, increase of jitter amplitude, and increase of jitter dispersion during a phase transition. We developed two different statistical methods for this analysis–*(i) KS-test method*, and *(ii) jitter dispersion method (JD)*. The first combines detection of changes on RTT latency baseline with the Kolmogorov-Smirnov (KS) test to detect changes in the jitter time series. The *jitter dispersion method (JD)* detects a jitter dispersion increase that correlates with a baseline RTT increases as a signal of congestion. The common goal of both methods is to objectively capture the signatures in the jitter signals. This section describes the role of each element of the Jitterbug framework in detail. We designed Jitterbug to support different RTT data sources, and have applied it to measurements collected by Ark CAIDA and RIPE Atlas. The current implementation uses a 5-minute and 15-minute granularity for RTT measurements and the aggregated minimum RTT time-series, respectively.

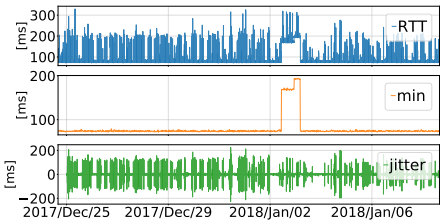
3.1 Signal filtering

Jitterbug congestion inferences use three signals: *(i) min* RTT time series, *(ii)* jitter, and *(iii)* jitter dispersion. As we saw in §2.2, raw RTTs can be too noisy

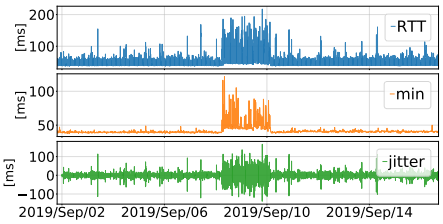


(a) Recurring congestion event. RTTs and jitter increase during congestion episodes.

(b) Recurring congestion event. Jitter does not significantly increase during elevated RTT periods, likely due to small buffer size in the bottleneck router.



(c) One-off non-congestion event on Jan 2. Jitter remained stable in face of inflated RTT.



(d) One-off congestion event. Increased varibility in jitter indicates the occurance of congestion.

Fig. 1. Typical examples of network events. The raw timeseries (top figures) is the raw RTT data with 5-minute resolution. We aggregate the raw data into 15-minute buckets with the minimum function to filter noise (middle figures). We compute jitter using the 15-minute aggregated data to quantify variability in RTTs (bottom figures).

to yield meaningful signatures. We first aggregate the raw RTT data by selecting the minimum value in each 15-minute time interval (*min* time series). The signal filtering module then computes the jitter using both the *raw RTT* and *min* time series to produce *jitter* and *j-min* time series, respectively.

We use two additional filters to better capture the variability in *j-min*. First, we apply the *Moving IQR filter* to the *j-min* time series, which computes the inter-quartile range (IQR) of a sliding window of 150 minutes (10 jitter samples). We define as jitter dispersion to the operation of computing the moving IQR to a jitter signal.

We then compute the 5-sample moving average of the resultant time series as the *jitter dispersion* time series to mitigate the impact of short-term latency spikes. Fig. 3 shows the correlation between the *min* RTT time series and the *jitter dispersion* of previous examples (Fig. 1). Correlation between the two time series in Fig. 3c) is low. We believe that the shift of baseline RTT corresponds to a route change that increased the propagation delay, which is a deterministic component that induces low variance to RTTs.

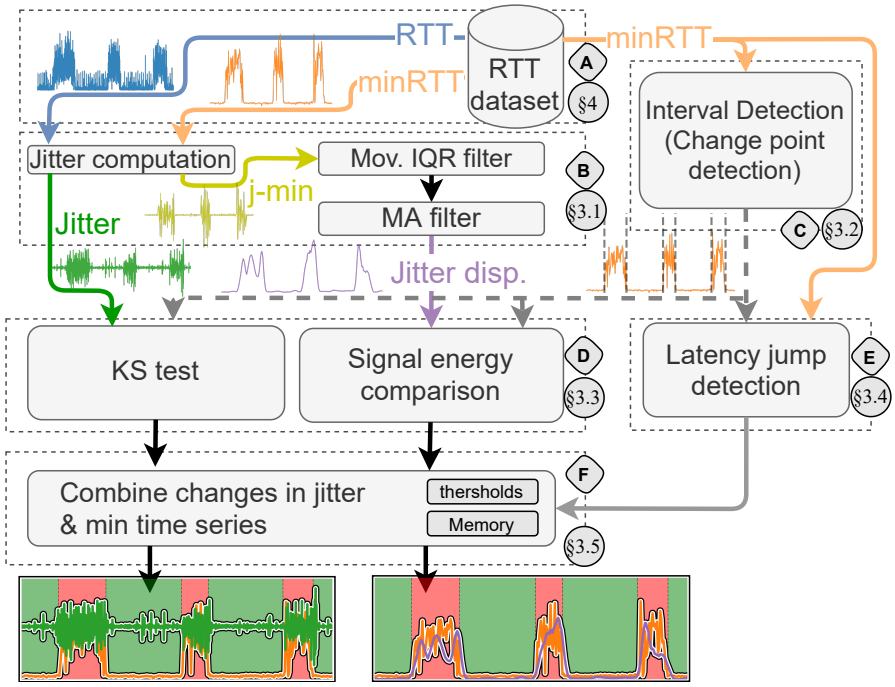
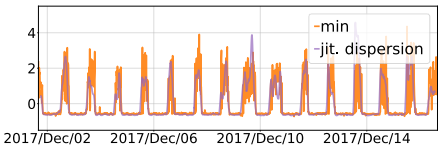


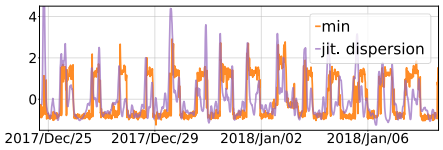
Fig. 2. The Jitterbug framework comprises: (A) data acquisition (B) signal filtering (C) detection of intervals of elevated latency (D) detection of changes of state of jitter and jitter dispersion signals (E) detection of increments of the min time series (F) correlation of changes in jitter state with increments of changes of state in jitter signals.

3.2 Detection of period of elevated latency

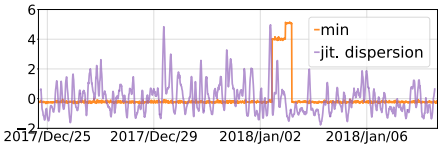
Identifying time intervals with elevated RTTs. is a fundamental step of the congestion inference process since the subsequent modules examine these periods to determine if latency elevations were caused by increases of traffic loads. Our framework can accommodate any change point detection algorithm that can segment time intervals based on changes in RTTs. As proof of concept, we use two state-of-the-art change point detection algorithms—Bayesian Change Point (BCP) Detection or Hidden Markov Models (HMM)—to process the *min* time series. We have not yet had the opportunity to test these methods on a large variety of data sources, so we provide both alternatives to let Jitterbug users select which is more effective for their data source. We believe these two algorithms can complement each other in circumstance where one fails to cover all change points in a signal. In §5.8, we test both algorithms with challenging latency signatures and show how all periods of elevated latency are captured by at least one of the methods.



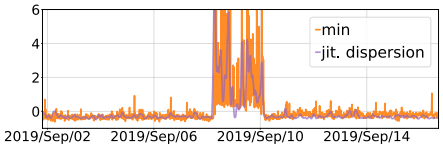
(a) Recurring congestion event. There is a correlation between periods of elevated latency and the growth of jitter dispersion.



(b) Recurring congestion event. Jitter dispersion transitorily increases at the beginning of periods of elevated latency



(c) One-off non-congestion event on Jan 2, with no correlation between signals.



(d) One-off congestion event, with a positive correlation between the *min* and jitter dispersion time series.

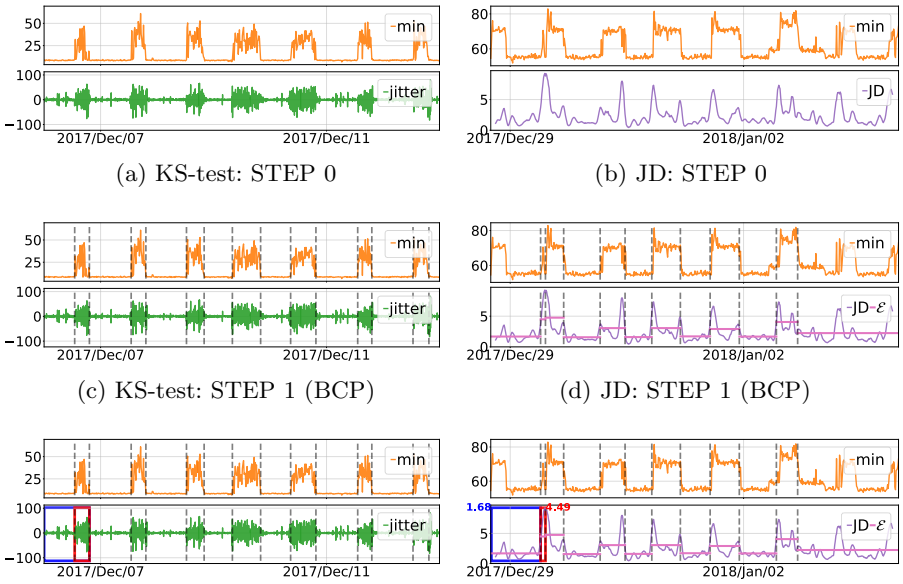
Fig. 3. *min RTT* (orange) and jitter dispersion (purple) time series. We normalized the values using standard score for this visualization; normalization is not necessary in actual computation. In Fig. 3a and 3d, these two signals are strongly correlated during period of congestion. In Fig. 3b, jitter dispersion has a transitory increase at the beginning of the period of elevated latency. Fig. 3c (no apparent congestion) shows no correlation between these signals, which is consistent with a route change that increased RTT.

- **Bayesian Change Point (BCP)**: We chose an offline BCP algorithm[6] proposed by Xuan *et al.* [36]. We experimented with other popular change point detection algorithms (e.g., Change finder [11] and ATDK LevelShift [6]) and found that BCP was the most effective at detecting boundaries of intervals with RTT latency measurements in our data.
- **Hidden Markov Models (HMM)**: We selected an implementation designed to identify different discrete states in RTT latency time series, by combining Hidden Markov Models (HMM) with Hierarchical Dirichlet Process (HDP) [27]. HMM also yields boundaries for each state (or level) in the time series, and in our case, consecutive RTT latency samples typically belong to the same state for long periods of times.

3.3 Examination of jitter signals

Jitterbug uses two approaches to examine changes in jitter and jitter dispersion time series during periods of elevated latency (Module (D) in Fig. 2): *(i) KS-test method* (using the jitter time series), and *(ii) Jitter dispersion method* (using the

[6] Implementation of Xuan *et al.* change point detection algorithm: https://github.com/hildensia/bayesian_changepoint_detection.



(a) KS-test: STEP 0 (b) JD: STEP 0

(c) KS-test: STEP 1 (BCP) (d) JD: STEP 1 (BCP)

(e) KS-test: STEP 2 (Compare intervals) (f) JD: STEP 2 (Compare intervals)

Fig. 4. Steps of KS-test (left) and jitter dispersion (right) congestion inference methods. In both methods, Jitterbug uses the *min* time series to identify the beginning and end of periods of elevated latency (Fig. 4c and Fig. 4d). Using these boundaries, both methods look for changes in jitter signals in adjacent intervals. To detect these changes, KS-test computes the Kolmogorov-Smirnov test on adjacent jitter samples (Fig. 4e); the jitter dispersion method (Fig. 4f) compares the mean value of the jitter dispersion signal ($\mathcal{E}$).

jitter dispersion time series). Both methods rely on boundaries previously identified by the Interval Detection Module (Module (C) in Fig. 2). Fig. 4 describes the input time series of each method, how they use change points detected by Interval Detection Module and how they detect changes in jitter signals.

KS-test method This method examines changes in the jitter time series (Fig. 4a). Using the change points extracted from the minimum time series by the Interval Detection Module (Fig. 4c), Jitterbug detects a change of regime in jitter time series during periods of elevated latency. Our hypothesis is that a trace switched into a different congestion state if there is a change point in the minimum time series and, at the same time, the jitter changes to a different regime. To identify such a regime, Jitterbug applies the Kolmogorov-Smirnov (KS) test to jitter samples in partitions before and after the change point (Fig. 4e). In case the jitter samples in the partition before the change point have a different distribution from the following partition, the KS test will reject the null hypothesis ($\alpha = 0.05$) meaning both samples were not generated by the same random

process. To verify that the result of the KS test is not an artifact due to the change point detection method, we apply the KS test to two random samples in the same interval. For this validation test, we expect the KS test does not reject the null hypothesis, which means there is no evidence to conclude that samples within the same partition belong to different jitter regimes. We repeat this process for all pairs of adjacent partitions.

Jitter dispersion method The input to this method is the jitter dispersion time series that we pre-computed in §3.1 (Fig. 4b). Similar to the KS-test method, this method uses change points extracted from the minimum time series by the Interval Detection Module (Fig. 4c), as boundaries between periods of elevated latency (Fig. 4d). We assume when the elevation of latency is caused by congestion, then the jitter dispersion increases, either transitorily at the beginning (phase transition) or throughout the period (§3.1).

In both cases, during a period of congestion the average jitter dispersion is larger than that of congestion-free periods. If the mean value of the jitter dispersion between consecutive periods (Fig. 4f) increases, we consider this period as congested. We repeat this inference process for all pairs of adjacent partitions.

3.4 Latency Jump Detection

Jitterbug assumes that *a period of congestion is a period of elevated latency* that manifests the growth of routers' buffers occupancy. In the Latency Jump Detection module (Module (E) in Fig. 2) Jitterbug uses the *min* time series and the intervals identified by the Interval Detection Module (Module (C) in Fig. 2) to detect latency increments. This modules flags a candidate *period of congestion* if it detects in that period an increment of the mean value of the *min* time series compared to its predecesor.

3.5 Combine changes in jitter and minimum time series

Jitterbug classifies a *period of congestion* (Module F in Fig. 2) if adjacent intervals meet two conditions: *(i)* an increase in the RTT latency baseline *(ii)* an increase in the jitter amplitude (transitory or generalized). Jitterbug combines the results obtained by the Latency Jump Detection module with KS-test and Jitter dispersion methods. Jitterbug assumes that a period of elevated latency was generated by an increase in routers buffer occupancy if the KS-test or jitter dispersion method detected changes in the jitter signals during that interval.

To increase the accuracy of these Jitterbug inferences in challenging scenarios, and to allow users to calibrate inferences with their tolerance values, Jitterbug includes two *additional features*: *(i) congestion inference thresholds*, and *(ii) memory*.

– **Congestion inference thresholds**. To increase confidence of Jitterbug congestion inferences, we include *congestion inference thresholds* when we

Table 1. Description of the near- and far-side ASes in the evaluation dataset. We use measurements collected from 13 Ark monitors hosted in 6 U.S. ISP to 18 far-side ASes (7 Content Providers and 11 Access/Transit networks) and 49 far-IP addresses. This data collection comprises 1.7M raw RTT samples collected between 2017 and 2020. for 1290 unique combinations of <day, VP, far IP>.

near-side ASes		far-side ASes	
# VPs	ISPs	#ASes (# addr.)	far ASname
13	COMCAST, Verizon, AT&T, CenturyLink, Charter, Cox	18 (49)	COMCAST (AS7922), Netflix (AS2906), NTT (AS2914), Level3 (AS3356), PCCW (AS3491), KT (AS4766), Telstra (AS4637), TATA (AS6453), China Telecom (AS4134), Zayo (AS6461), Cloudflare (AS13335), Charter (AS7843), XO (AS2828), Edgecast (AS15133), Google (AS15169), Amazon (AS16509), Akamai (AS20940), Facebook (AS32934)

compare the mean value of the minimum RTT time series of consecutive intervals. We also include a Jitter dispersion threshold (JD threshold) in the jitter dispersion method when we compare changes in the mean value of the signal in adjacent intervals. The values we use for this research are 0.25ms and 0.5ms thresholds for jitter dispersion and baseline, respectively, as we found in the evaluation dataset (see § 4) that min and jitter dispersion fluctuations tend to be below these values during periods of no suspected congestion. These parameters allow us to reduce false positives and false negatives in Jitterbug congestion inferences.

– **Memory**. To reduce errors in congestion inferences as a result of false positives in the change point detection process, we include the concept of *memory*. In some cases, change point detection algorithms identify path anomalies within periods of congestion (e.g., route change during a congestion episode) or a false positive. Under these circumstances, our congestion detection methodology would not detect any change, either transitory or permanent in the jitter, and it would label the next interval as a *period of no congestion*. However, the congestion status has not changed between these adjacent intervals. To overcome this limitation, we include a rule called *memory* that assumes that *a period of congestion has not finished if in the following interval the mean value of the minimum RTT does not decrease*. For example, for two given adjacent intervals I_1 and I_2, we will label I_2 as *a period of congestion* if we also labeled I_1 as *a period of congestion* and $mean(minRTT(I_2)) \geq mean(minRTT(I_1))$.

4 Dataset

We focus on congestion at interdomain links which requires identification of IP addresses of intedomain routers' interfaces. MANIC [2] uses *bdrmap* [24] to infer

the IP addresses of all interdomain links visible from the Autonomous System hosting a CAIDA Ark [1] vantage point (VP). *bdrmap* returns pairs of near- and far-side IP addresses of an interdomain link, and a set of prefixes reachable through a path containing those near- and far-side IP addresses. We use the data API of the MANIC platform [2] to obtain longitudinal RTT measurements from Ark's VPs to the far-side interface of interdomain links using the Time-Series Latency Probing (TSLP) method [23]. Each VP runs TSLP measurements every 5 minutes using ICMP TTL-limited packet probes to all near- and far-side pairs to collect RTT samples between the VP and IP addresses on the near and far side of interdomain links. Furthermore, the MANIC platform labels interdomain links that might have congestion events using an autocorrelation-based method [12], which is effective in locating recurring congestion events that significantly inflate the RTTs. We will use these inferences as cross-validation (§6.2).

We demonstrate our methodologies by inferring congestion from 13 VPs in 6 U.S. ISPs to 18 far ASes and 49 far-IP addresses, as it is shown in Table 1. This dataset covers a total of 1290 unique combinations of <day, VP, far IP> and contains 1.7M raw RTT samples collected between 2017 and 2020.

5 Results

We present our results of Jitterbug congestion inferences in the scenarios we introduced in §2.2, which map to the taxonomy in Fig. 5. Specifically, we show Jitterbug congestion inferences for periodic signals of large (§5.1) and small (§5.2) amplitude as well as for one-off periods of elevated latency (§5.3 and 5.4). We further investigate Jitterbug congestion inference in hybrid scenarios with one-off events in the middle of repetitive periods of elevated latency (§5.5). We also study the impact of *memory* (§5.6) and the *JD threshold* (§5.7) in the accuracy of Jitterbug congestion inferences. Finally, we investigate how errors in detecting change points impact in Jitterbug congestion inference (§5.8).

5.1 Scenario 1: recurrent period of elevated latency with large amplitude signals

Both methodologies labeled every recurrent period of elevated latency as a period of congestion (Fig. 6). We suppose that the accuracy of the congestion inferences is partially due to the small of contribution of other random factors since we observe small variability in the baseline during periods of non-elevated latency. The profile of the minimum time series indicates a small contribution of other random components, which create slight fluctuations during periods of non-elevated latency. In addition, the size of this router buffer amplifies the range of the raw, min and jitter time series (in some cases over 100ms) which simplifies the task of identifying periods of high jitter fluctuations.

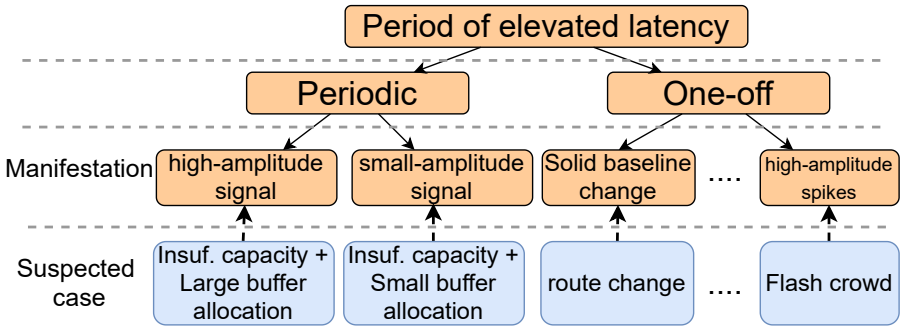


Fig. 5. Hierarchical classification of characteristics of elevated latency. We classify periods of elevated latency as either *periodic* (left branch) or *one-off* (right branch). Recurrent latency with a consistent period (periodic) suggests an underprovisioned link. A one-off episode of elevated latency can have many causes, e.g., bufferbloat, flash crowd, misconfiguration, route change.

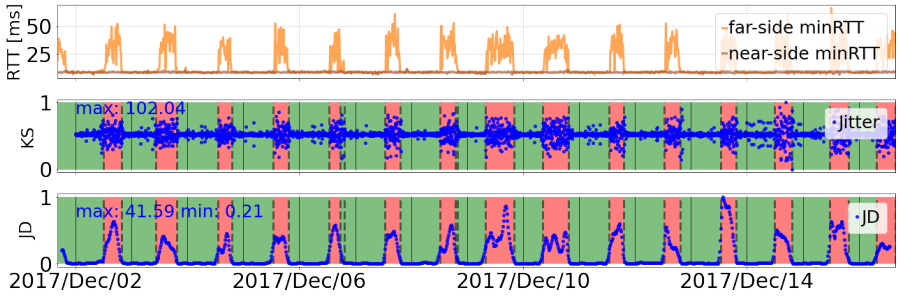


Fig. 6. KS-test (middle plot) and Jitter dispersion (lower plot) congestion inferences for a periodic high-amplitude signal. In this case, both methods label every recurrent period of elevated latency as periods of congestion. Red-filled intervals indicate periods of congestion.

5.2 Scenario 2: recurrent period of elevated latency with small amplitude signals

Fig. 7 shows that only the jitter dispersion method labels periods of elevated latency as periods of congestion. We believe that the stability in the jitter time series at periods of elevated latency impedes the KS-test method's inferences. This jitter stability may be due to small buffers (differences between peak and valley values is 30ms) or traffic engineering on the far side network, which in this case is a large Content Provider. On the other hand, the high amplitude of the phase transitions in the jitter dispersion time series allows the JD method to detect differences in the mean value of this signal during periods of elevated latency. We note that the change point detection module is not capable of detecting period of elevated latency between January 1, 2018 and January 3, 2018.

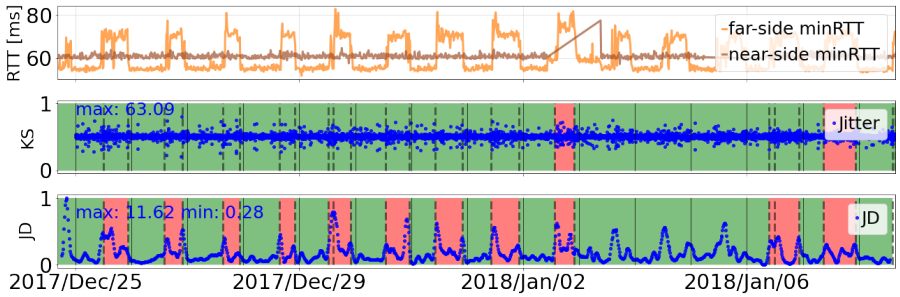


Fig. 7. KS-test and Jitter dispersion congestion inferences for a periodic small-amplitude signal. Only the jitter dispersion method infers congestion from this recurrent pattern, which we speculate relates to small buffers that keep jitter itself relatively stable. Remarkably, the change point detection algorithm was not able to capture some periods of elevated latency. Red-filled intervals indicate periods of congestion.

(The slightly smoother transition during this period trace could have hindered the accuracy of the change point detection algorithm.)

5.3 Scenario 3: one-off period of elevated latency with no congestion

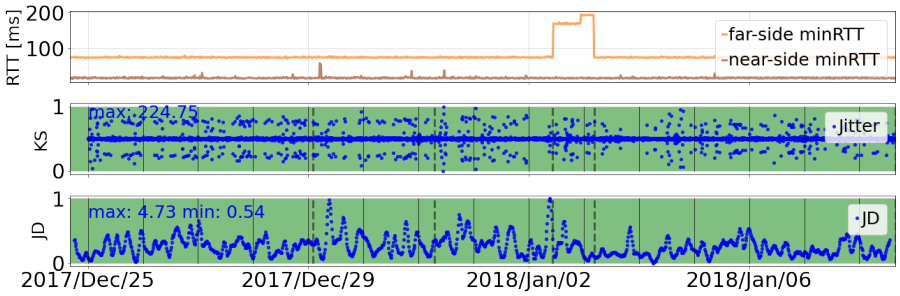


Fig. 8. KS-test and Jitter dispersion congestion inferences for a one-off event suspected as a route change. Inferences for this case indicate no congestion. Red-filled intervals indicate periods of congestion.

Fig. 8 shows an example in which neither method infers congestion. In this case, we do not observe any change in either the jitter time series or the jitter dispersion either before or after the period of elevated latency. We suppose that this period corresponds to a route change based on the stability of the jitter time series and the clean profile of the min time series during the transition. Since there is no simultaneous increase in near-side RTT (orange curve in Fig. 8

top panel), we believe that a route changed in the reverse path from the far-side router.

5.4 Scenario 4: one-off period of elevated latency with congestion

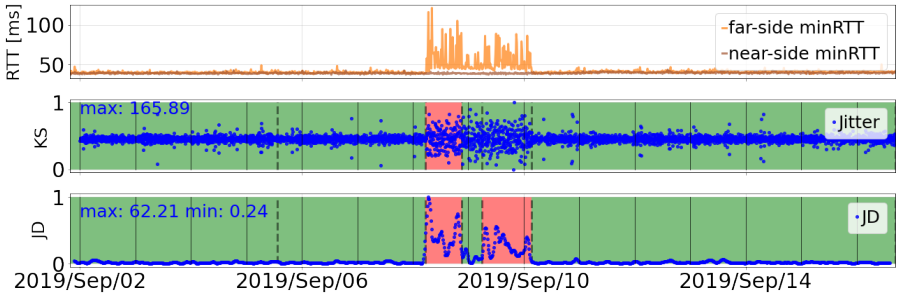
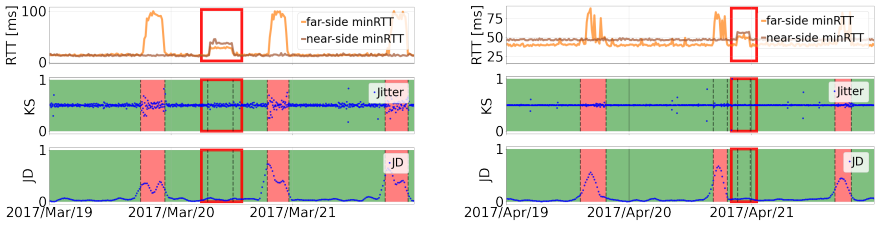


Fig. 9. KS-test and Jitter dispersion congestion inferences for a one-off congestion event. In this case, both methods infer congestion during periods of elevated latency. Red-filled intervals indicate periods of congestion.

(Fig. 9) Congestion inferences from both methods partially agree on classifying this one-time episode of high amplitude latency spikes as a period of congestion. Detection of multiple change points, and the fact that the period in between has slightly smaller mean value in the min time series, generate that the period of congestion inferred is smaller than the actual period of elevated latency.

5.5 Scenario 5: one-off event during recurrent periods of elevated latency

The biggest challenge for latency-based congestion detection is to distinguish congestion-induced elevated latency from other path anomalies, such as a route change. Fig. 10 shows two examples of KS-test and jitter dispersion congestion inferences when route changes occur in the middle of recurrent periods of elevated latency. In these cases, we confirm that the events occurring on March 20, 2017 at 12pm (Fig. 10a) and on April 20, 2017 before midnight (Fig. 10b) are route changes in the internal network of the ISP since the near- (orange) and far-side (blue) *min* time series detect an elevation simultaneously. As we expected for a route change, these events do not show any change in jitter signals. Our method used the jitter dispersion metric to correctly rule out a candidate congestion period as a route change (rather than congestion), due to low jitter dispersion which we know is not strongly correlated with congestion dynamics. This example illustrates the importance of jitter dynamics in detection of network congestion events.



(a) (b)

Fig. 10. Two examples of suspected route changes in the middle of recurrent periods of elevated latency. Neither method inferred any congestion. Red-filled intervals indicate periods of congestion.

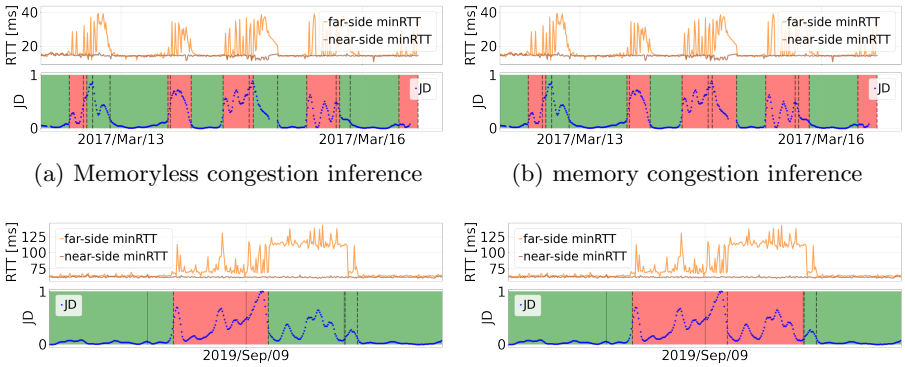
5.6 Scenario 6: Change point detection over-detects change points

We use an additional set of examples to investigate how the *memory* feature compensates for weaknesses in change point detection algorithms, specifically when algorithms are over-sensitive and create too many intervals.

Fig. 11 shows examples of how *memory* improves the accuracy of congestion inferences in different circumstances. Fig. 11a and 11b shows how *memory* increases the accuracy of congestion inferences in the presence of over-partitioned periods of elevated latency. While this feature increases the number of intervals labeled as periods of congestion in the presence of multiple change points, it is not able to fix all of them. Fig. 11c and 11d show how *memory* extends the inferred period of congestion where there is a legitimate change point during this period. These figures show a persistent increase in the minimum RTT baseline, which we suspect was due to a route change during a period of congestion. We assume that the lack of RTT measurements below that baseline corresponds to speed-of-light constraints induced by the more circuitous path used during the period of congestion.

5.7 Scenario 7: Adjusting JD threshold to minimize false positives

Fig. 12 shows examples of how one can adjust the JD threshold to minimize false positives in congestion inferences. Fig. 12a and 12b compare congestion inferences using JD thresholds of 0.25 ms and 0.5 ms, respectively. In this example, the jitter dispersion ranges from 0.26 to 92.64 ms, showing a flat curve for most of the period and a one-off event that generates a large spike. Due to the flatness of the curve we selected two thresholds close to the baseline jitter dispersion values (D+0.25 and D+0.5 ms), and inferred a period of congestion if jitter dispersion exceeded these thresholds, which in this case means the jitter dispersion doubled or tripled. We found that our first threshold (0.25) was too sensitive, since a small perturbation in jitter dispersion, in addition to a false positive inference from the change point algorithm, generated a false positive congestion inference.



(a) Memoryless congestion inference

(b) memory congestion inference

(c) Memoryless congestion inference

(d) Memory congestion inference

Fig. 11. Examples of how the *memory* feature improves accuracy of congestion inferences in the presence of of over-partitioned intervals and other path anomalies. Fig. 11a and 11b display how *memory* maximizes congestion inferences in scenarios where change point detection algorithms overfit detection, breaking the time series into too many intervals. Fig. 11c and 11d show another example of how *memory* can inform congestion inference when a route change occurs within a period of congestion. Red-filled intervals indicate periods of congestion.

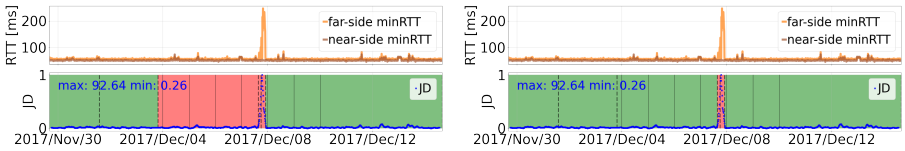
5.8 Scenario 8: False negatives in change point detection

One desired characteristic of a change point detection algorithm is the ability to precisely detect the beginning and ending points (all of them) of *all* periods elevated latency. In practice this is not possible for every time series, and in our case the lack of change points hinder the accuracy of congestion inferences. We use additional examples to investigate the accuracy of the change point detection algorithms we included in Jitterbug.

Fig. 13 shows two pairs of examples where the precision of Interval Detection varies depending on the algorithm being applied and the traffic scenario: BCP is more precise that HMM (Fig. 13a and 13b) and HMM is more precise than BCP (Fig. 13c and 13d)). Fig. 13a shows a scenario where HMM misses several consecutive change points, creating a prolonged period that does not precisely capture the periods of congestion in that measurement. For the same scenario, Fig. 13b shows that BCP correctly infers those periods of congestion. Conversely, Fig. 13c shows a scenario in which HMM is more accurate than BCP at detecting change points (Fig. 13d).

6 Comparative evaluation of Jitterbug

The current version of Jitterbug allows users to infer congestion using 4 different configurations by changing: *(i)* the change point detection algorithm (BCP or HMM, see §3.2), or *(ii)* the congestion inference method (KS-test or jitter



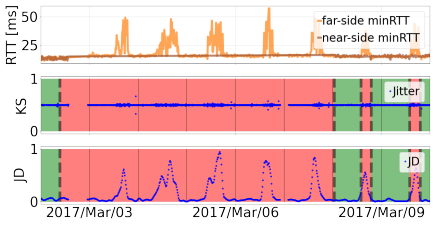
(a) JD threshold = 0.25 ms (b) JD threshold = 0.5ms

Fig. 12. Adjusting the JD threshold can mitigate false positive in congestion inferences. Fig. 12a shows that a too-sensitive threshold can yield errors even in the presence of a flat jitter dispersion time series. Fig. 12b shows how small adjustments in this threshold can mitigate false positive congestion inferences. Red-filled intervals indicate periods of congestion.

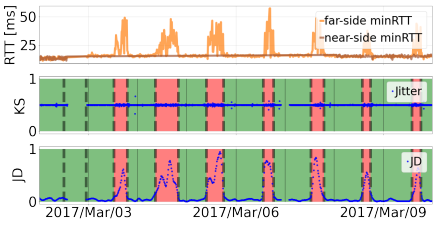
dispersion, see §3.3). In this section we compare Jitterbug inferences for each configuration, first comparing the KS-test and JD methods to each other (§6.1), and cross-validated with the state-of-the-art congestion detection methods [12] (§6.2).

6.1 Comparing inferences of KS-test and JD methods

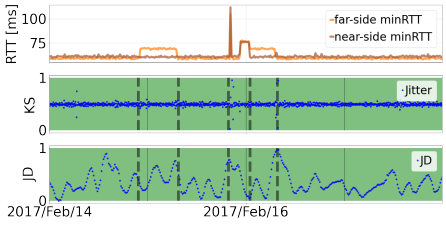
Table 2 compares congestion inferences of KS-test and jitter dispersion methods for the same interval using different change point detection alternatives (BCP on the left hand-side and HMM on the right hand-side). The results show no significant variations related to the change point detection used for the inferences. KS-test and jitter dispersion indicate the same congestion status for most intervals since the fraction of intervals equally labelled is 0.67 (128/192) and 0.64 (129/201) when using BCP and HMM, respectively. The jitter dispersion method tends to label more intervals as *period of congestion* than the KS-test method where the fraction of intervals considered as *periods of congestion* only by jitter dispersion is 0.29 (56/192) and 0.32 (63/201) for BCP and HMM, respectively. The KS-test method labels fewer intervals as *period of congestion* since this method only detects a narrow type of congestion signature in which congestion implies a change in jitter regime. For instance, when random components of latency are more significant than queueing delay, this noise limits the ability of KS-test to detect a change in the jitter regime. In addition, we found that the KS-test is unable to detect congestion generating changes of jitter regimes when a bottleneck router buffer is small. We suspect that small buffers do not allow us to observe jitter fluctuations to classify them as a change of jitter regime. Active traffic engineering strategies could keep jitter within a certain band. Despite that the KS-test method effectively infers congestion for a narrow type of congestion signature, we have included this method for its simplicity to detect congestion in cases with a large signal-to-noise ratio.



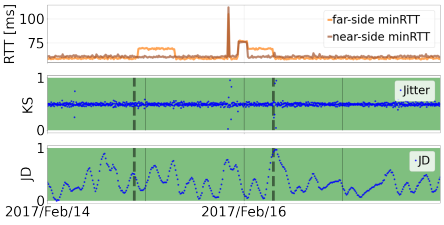
(a) Example A: HMM misses some change points



(b) Example A: BCP detects all change points



(c) Example B: HMM detects more change points than BCP (Fig. 13d)



(d) Example B: BCP misses some change points

Fig. 13. Two pairs of examples showing the limitations of change point detection algorithms to detect *all* change points (vertical dashed lines). Fig. 13a shows an example where HMM is not able to capture some change points in contrast to BCP that detects all of them (Fig. 13b). Fig. 13c shows an example where HMM is a more accurate than BCP at detecting change points (Fig. 13d) Red-filled intervals indicate periods of congestion.

6.2 Comparing inferences with cross-validation data

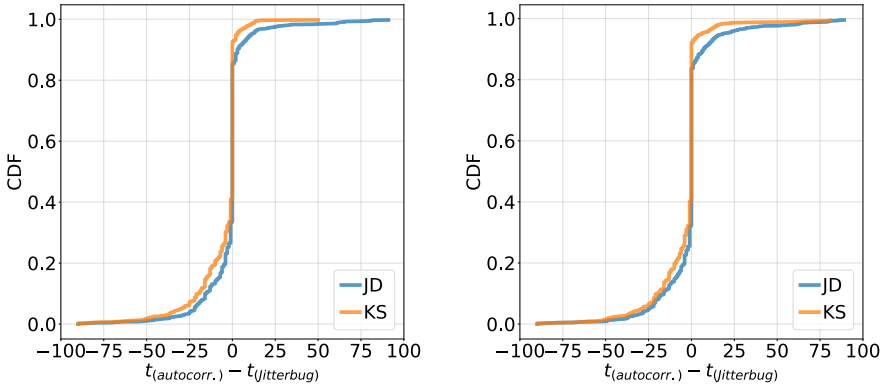
We validate KS-test and jitter dispersion congestion inferences using CAIDA's autocorrelation-based congestion inferences as cross-validation data. In the presence of recurrent congestion, CAIDA's congestion inferences count the number of 15-minute intervals with elevated latency. Using this schema, CAIDA's congestion inferences report the daily congestion severity of a link with a variable that ranges from 0 to 96[7]. We use Jitterbug outputs to generate the same daily estimations.

Fig. 14 shows how close are the daily congestion estimations of Jitterbug and CAIDA's congestion inference data. We also compared estimations with a maximum difference of 10% (in number of congested 15-minute intervals), and the fraction of days that agree to within this 10% margin rises to 76-80% depending on the combination (80% for JD method using BCP). The most prominent discrepancies in this evaluation corresponds to two categories: *(i)* Jitterbug false positive inferences in periods with no congestion, and *(ii)* one-off congestion

[7] One day has 96 periods of 15 minutes.

Table 2. Fraction (and total number) of (dis)agreements for different methodologies. The bar on top means a scenario with no congestion.

	BCP			HMM		
	$\overline{C_{KS}}$	C_{KS}	**SUM**	$\overline{C_{KS}}$	C_{KS}	**SUM**
$\overline{C_{JD}}$	0.43 (82)	0.04 (8)	0.47 (90)	0.39 (80)	0.04 (9)	0 .43 (89)
C_{JD}	0.29 (56)	0.24 (46)	0.53 (92)	0.31 (63)	0.24 (49)	0.57 (112)
SUM	0.72 (138)	0.28 (54)	**192**	0.70 (143)	0.28 (58)	**201**



(a) BCP (b) HMM

Fig. 14. Cumulative distribution function of the differences between the estimated daily time of congestion by autocorrelation-based methods and Jitterbug. These methods show remarkable similarity: 52% of days show no difference in inference regardless of change point detection method or congestion-detection method (KS vs JD).

events detected by Jitterbug but not present in CAIDA's congestion inference data since CAIDA's method only attempts to infer recurrent (periodic) congestion episodes.

7 Lessons learned

In this section we enumerate important aspects we have identified for jitter-based congestion inference.

1. **Jitter and jitter dispersion signatures provide meaningful information to identify congestion events as periods of elevated latency**. We found that periods of congestion manifest in RTT latency measurements not only as periods of elevated latency, but also changes in jitter (and jitter-derivated signals) time series.

2. **Jitter signals allowed us to discard periods of elevated latency generated by other path anomalies, e.g., route changes**. Including jitter-based analysis in the detection of congestion events allowed us to differentiate congestion events from other path anomalies. In non-congestion-related events, jitter and jitter dispersion time series tend *not* to change during periods of elevated latency.
3. **Period of elevated latency only to the far-side does not necessarily mean congestion**. We noticed that the simultaneous periods of elevated latency to near- and far-sides suggest a route change in the internal network of the ISP but a period of elevated latency to the far-side only does not necessarily indicate congestion. Although in many cases a period of elevated latency to the far-side only indicates a growth in the buffer occupancy of the interdomain link, this event could also suggest a route change only in the reverse path from the far-side router. We use jitter and jitter dispersion to identify traces with elevations only to the far-side router but not corresponding to congestion events.
4. **Shallower increments of RTT values when a link transitions to a period of congestion tend to affect jitter signatures too**. We observed a negative correlation between the increment of RTT values during periods of congestion and the visibility of changes in jitter signatures. We suppose this decrement in the contrast of RTT latency values between periods of elevated latency and other periods is related to the size of router buffers. We speculate that modern recommendations to keep buffers small [5] will likely affect jitter time series.
5. **The contribution of other random components of RTT latency can reveal congestion dynamics** . Some traces contain random contributions that mask queueing delay fluctuations in the jitter time series during periods of elevated latency. Although this is not a widespread phenomenon, it could compromise Jitterbug's ability to infer congestion, especially with the KS-test method.
6. **Limitations of change point detection methodologies to detect *all* periods of elevated latency**. None of the change point detection algorithms we examined could identify all change points in the *min* time series in our data. There is a wide variety of signal profiles in RTT latency measurements and several types of congestion signatures, including periods of elevated latency with flat, smooth and spiky signatures. We suppose that change point detection algorithms may not be able to capture change points for all types of signatures in this large set of profiles. To be able to identify *all* periods of elevated latency is crucial since the accuracy of Jitterbug congestion inferences mostly relies on detecting these intervals.
7. **Change point detection is expensive**. The BCP and HMM methods required significant time to execute on the 15-day traces we analyzed for this study, typically between 60 and 90 seconds. Optimizing performance of these methods will be critical for operational utility.
8. **The KS-test method only captures a limited type of congestion event signature**. But it is a simple and clean congestion inference approach,

cost-effective for many scenarios beyond those we studied, and can inform further research in this area.

8 Related work

Inferring network congestion with RTT measurements. Previous research efforts focused on interdomain congestion inference leveraging from recurrent periods of elevated latency [12,23]. To generate these inferences, these works relied on a set of CAIDA's (Ark) [1] to run RTT latency measurements to all visible IP-level interconnection links [24]. Time Series Latency Probes (TSLP) [12,23] is the result of these latency measurement campaigns. An autocorrelation method is apply to traces on the TSLP data collection to find multi-day repetition of elevated delays around the same times, i.e., driven by diurnal demand. However, this method to detect congestion requires some level of manual inspection. With a similar approach, Fontugne *et al.* [15] proposed a latency-based methodology to detect congestion in last-mile access networks. They used RIPE Atlas probes to run traceroute measurements campaigns and inferred congestion applying a methodology to detect latency deviations.

Anomaly detection on network paths. RTT time series has been also used to detect a wide range of network events, such as path anomalies [13,14] and route changes [30,17].

Change point detection. Change Point Detection algorithms aim to detect *change point detection* (also known as time series segmentation) as abrupt changes in a sequence of observations (e.g., a time series) to divide a sequence into a finite number of non-overlapping partitions [3]. These algorithms are typically based on mathematical or machine learning models [3,4,11,31,36]. Another study found that some unsupervised anomaly detection tools for change point are notably time consuming [32]. Even though these methods are effective in capturing change points in the time series [9], event classification still requires human inspection.

Mathematical approaches for congestion detection. Another type of studies brought sophisticated mathematical and statistical concepts to investigate congestion events. Mouchet *et al.* [27] proposed to use Hidden Markov Models (HMM) to identify different states in RTT latency time series, however, these states correspond to different latency values and do not report discriminate events caused by different types of events (e.g., route change vs congestion event). More recently, Spang *et al.* [34] proposed to use A/B tests in TCP lab measurements to generate unbiased evaluations of TCP Congestion Control Algorithms (CCA). However, the applicability of this approach relies on the assumption on independent traffic flows, which in practice may be compromised by the synchronization of TCP flow and short-lived TCP transfers. In addition, engineers typically used more pragmatic evaluations to test the impact of their changes.

9 Open Challenges

Other approaches not covered in this paper may be useful to extract information embedded in jitter signals. Early in this project we proposed and tested at least other four different approaches to jitter-based congestion inference. One aimed to capture the jitter variability at the beginning of a period, and another applied the same concept of the KS-test method but using j-min (definition in §3.1) instead. A third alternative used anomaly detection techniques to detect changes in jitter volatility. The fourth alternative used parametric models, including Normal and Levy-Stable distributions, to fit jitter behavior. These alternative approaches are promising and it is worth exploring them as part of future work.

In the future we also expect fluctuations of queueing delay to become more challenging to distinguish in RTT latency measurements as a consequence of smaller router buffers following modern buffer sizing recommendations [5,16]. Jitterbug central assumption is that *a period of congestion is a period of elevated latency*, however, if latency signatures show imperceptible queueing delays, this may comprise the accuracy of change point detection algorithms to detect periods of elevated latency. In addition, the rise of delay-sensitive real-time applications (e.g., videocalls, online gaming, etc.) could also incentivize the reduction of router buffer sizes. We observed (§2.2) a correlation between jitter signatures and buffer sizes and recognize that smaller buffer sizes could impede Jitterbug congestion inferences.

More demanding requirements of jitter-sensitive applications (e.g. live video streaming) could also modify traffic patterns and latency signatures. Today's HTTP-based video delivery relies on playback modulation to mitigate jitter impact on video flow [28,29]. However, in the future, real-time video broadcasting may requiere shorter playback jitters — and consequently dedicated traffic engineering strategies — that could modify the shape of the jitter curve and thus Jitterbug inferences.

Foreseeable changes in the foundational protocols of the TCP/IP stack could modify traffic dynamics and the nature of latency signatures. New latency-based Congestion Control Algorithms could modify latency signatures and buffer occupancy. The rollout of QUIC [22,8,33,18] could spread new features in the network potentially reshaping the nature of traffic dynamics. For example, QUIC proposes to aggregate and multiplex multiple short-lived web data transfers — typically run in parallel per-resource TCP sessions [8]— into a single transport-layer protocol session.

We expect that future work from ML/AI communities develop more cost-effective change point detection tools. The growing necessity of monitoring large-scale time series databases to generate (near) real-time anomaly detection is likely to be the driver of optimization in this space [32]. We expect that in the coming years we are going to count with more rapid and optimized supervised and unsupervised anomaly detection algorithms to detect change points.

10 Conclusions and Future work

In this paper we proposed Jitterbug, a novel framework to infer network congestion combining pre-existing approaches with information embedded in jitter signals. We found that jitter allowed us to expand congestion inference beyond scenarios of recurrent congestion patterns, such as one-time congestion events. We discovered that jitter (and jitter-derived signals) time series is useful to discriminate periods of elevated latency caused by congestion from route changes.

We have also learned about the various challenges of inferring network congestion with RTT latency measurements. The vastly heterogeneous structure of the network is reflected in diverse latency signatures showing large and short buffer sizes, remarkable presence of randomness unrelated from congestion events, etc. We have also learned about limitations of change point detection algorithms in detecting all beginning and ending points of periods of elevated latency as well as the time required to obtain results from these algorithms.

Applying Jitterbug to the cases in our dataset, we obtained similar results to recent autocorrelation methods [12]. However, in contrast to that method, which is based on the repetitiveness of the signal and uses information of near- and far-side RTT latency measurements, Jitterbug is fully based on far-side RTT latency measurements and does not rely on repetitiveness to discern the congestion status of a period.

We hope that this work will encourage studies focused on network congestion inference, jitter analysis and change point detection algorithms. In the future, we would like to investigate how sampling rates (higher and lower) affect congestion inferences and profiles of RTT latency signatures. For example, studies in financial time series have found that the distribution of assets returns vary depending on the scaling factor (i.e. time elapsed between samples) [20,25], we would like to investigate if this also happens on jitter time series. We are also interested in studying whether we could develop purely jitter-based congestion inference methods. Another topic that we would like to investigate is if inter-packet delay in back-to-back measurements, for example using FAST probing tool [26], could allow us to infer congestion

11 Acknowledgements

We thank the anonymous reviewers for their insightful comments, and Maxime Mouchet for providing an implementation of the HMM algorithm. We would like to thank Fabian Bustamante (Northwestern University) for coming up with the original term *Jitterbug* to name this paper. This work was partly funded by research grants DARPA HR00112020014, NSF OAC-1724853 and NSF CNS-1925729.

References

1. Archipelago measurement infrastructure updates. https://catalog.caida.org/details/media/2011_archipelago, accessed: 2021-9-30

2. Manic. https://catalog.caida.org/details/software/manic, accessed: 2021-10-13
3. Adams, R.P., MacKay, D.J.: Bayesian online changepoint detection. arXiv preprint arXiv:0710.3742 (2007)
4. Aminikhanghahi, S., Cook, D.J.: A survey of methods for time series change point detection. Knowledge and information systems **51**(2), 339–367 (2017)
5. Appenzeller, G., Keslassy, I., McKeown, N.: Sizing router buffers. ACM SIGCOMM Computer Communication Review **34**(4), 281–292 (2004)
6. ARUNO: ADTK Detectors. https://arundo-adtk.readthedocs-hosted.com/en/stable/api/detectors.html (2021)
7. Cardwell, N., Cheng, Y., Gunn, C.S., Yeganeh, S.H., Jacobson, V.: Bbr: Congestion-based congestion control: Measuring bottleneck bandwidth and round-trip propagation time. Queue **14**(5), 20–53 (2016)
8. Carlucci, G., De Cicco, L., Mascolo, S.: Http over udp: an experimental investigation of quic. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing. pp. 609–614 (2015)
9. Davisson, L., Jakovleski, J., Ngo, N., Pham, C., Sommers, J.: Reassessing the constancy of end-to-end internet latency. In: Proceedings of IFIP TMA (2021)
10. Demichelis, C., Chimento, P.: Rfc3393: IP packet delay variation metric for IP performance metrics (IPPM). https://datatracker.ietf.org/doc/html/rfc3393 (Nov 2002)
11. Desobry, F., Davy, M., Doncarli, C.: An online kernel change detection algorithm. IEEE Transactions on Signal Processing **53**(8), 2961–2974 (2005)
12. Dhamdhere, A., Clark, D.D., Gamero-Garrido, A., Luckie, M., Mok, R.K., Akiwate, G., Gogia, K., Bajpai, V., Snoeren, A.C., Claffy, K.: Inferring persistent interdomain congestion. In: Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication. pp. 1–15 (2018)
13. Fontugne, R., Mazel, J., Fukuda, K.: An empirical mixture model for large-scale RTT measurements. In: Proceedings of IEEE INFOCOM (2015)
14. Fontugne, R., Pelsser, C., Aben, E., Bush, R.: Pinpointing delay and forwarding anomalies using large-scale traceroute measurements. In: Proceedings of ACM Internet Measurement Conference (2017). https://doi.org/10.1145/3131365.3131384
15. Fontugne, R., Shah, A., Cho, K.: Persistent last-mile congestion: Not so uncommon. In: Proceedings of the ACM Internet Measurement Conference. pp. 420–427 (2020)
16. Gettys, J.: Bufferbloat: Dark buffers in the internet. IEEE Internet Computing **15**(3), 96–96 (2011)
17. Iodice, M., Candela, M., Battista, G.D.: Periodic path changes in RIPE Atlas. IEEE Access **7**, 65518–65526 (2019). https://doi.org/10.1109/access.2019.2917804
18. Iyengar (Ed.), J., Thomson (Ed.), M.: QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000 (Proposed Standard) (May 2021). https://doi.org/10.17487/RFC9000, https://www.rfc-editor.org/rfc/rfc9000.txt
19. Jacobson, V.: Congestion avoidance and control. ACM SIGCOMM computer communication review **18**(4), 314–329 (1988)
20. Jaroszewicz, S., Mariani, M.C., Ferraro, M.: Long correlations and truncated levy walks applied to the study latin-american market indices. Physica A: Statistical Mechanics and its Applications **355**(2-4), 461–474 (2005)
21. Laki, S., Mátray, P., Hága, P., Csabai, I., Vattay, G.: A detailed path-latency model for router geolocation. In: EAI Tridentcom. IEEE (2009). https://doi.org/10.1109/tridentcom.2009.4976258
22. Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., Yang, F., Kouranov, F., Swett, I., Iyengar, J., et al.: The quic transport protocol: Design and

internet-scale deployment. In: Proceedings of the conference of the ACM special interest group on data communication. pp. 183–196 (2017)
23. Luckie, M., Dhamdhere, A., Clark, D., Huffaker, B., Claffy, K.: Challenges in inferring internet interdomain congestion. In: Proceedings of the 2014 Conference on Internet Measurement Conference. pp. 15–22 (2014)
24. Luckie, M., Dhamdhere, A., Huffaker, B., Clark, D., Claffy, K.: Bdrmap: Inference of borders between ip networks. In: Proceedings of the 2016 Internet Measurement Conference. pp. 381–396 (2016)
25. Mantegna, R.N., Stanley, H.E.: Econophysics: Scaling and its breakdown in finance. Journal of statistical Physics **89**(1), 469–479 (1997)
26. Marder, A., Claffy, K.C., Snoeren, A.C.: Inferring cloud interconnections: Validation, geolocation, and routing behavior. In: International Conference on Passive and Active Network Measurement. pp. 230–246. Springer (2021)
27. Mouchet, M., Vaton, S., Chonavel, T., Aben, E., Den Hertog, J.: Large-scale characterization and segmentation of internet path delays with infinite hmms. IEEE Access **8**, 16771–16784 (2020)
28. Mustafa, I.B., Nadeem, T.: Dynamic traffic shaping technique for http adaptive video streaming using software defined networks. In: 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). pp. 178–180. IEEE (2015)
29. Pu, W., Zou, Z., Chen, C.W.: Video adaptation proxy for wireless dynamic adaptive streaming over http. In: 2012 19th International Packet Video Workshop (PV). pp. 65–70. IEEE (2012)
30. Pucha, H., Zhang, Y., Mao, Z.M., Hu, Y.C.: Understanding network delay changes caused by routing events. ACM SIGMETRICS Performance Evaluation Review **35**(1), 73–84 (jun 2007). https://doi.org/10.1145/1269899.1254891
31. Punskaya, E., Andrieu, C., Doucet, A., Fitzgerald, W.J.: Bayesian curve fitting using mcmc with applications to signal segmentation. IEEE Transactions on signal processing **50**(3), 747–758 (2002)
32. Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., Xing, T., Yang, M., Tong, J., Zhang, Q.: Time-series anomaly detection service at microsoft. In: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. pp. 3009–3017 (2019)
33. Rüth, J., Poese, I., Dietzel, C., Hohlfeld, O.: A first look at quic in the wild. In: International Conference on Passive and Active Network Measurement. pp. 255–268. Springer (2018)
34. Spang, B., Hannan, V., Kunamalla, S., Huang, T.Y., McKeown, N., Johari, R.: Unbiased experiments in congested networks. arXiv preprint arXiv:2110.00118 (2021)
35. Turkovic, B., Kuipers, F.A., Uhlig, S.: Interactions between congestion control algorithms. In: 2019 Network Traffic Measurement and Analysis Conference (TMA). pp. 161–168. IEEE (2019)
36. Xuan, X., Murphy, K.: Modeling changing dependency structure in multivariate time series. In: Proceedings of the 24th international conference on Machine learning. pp. 1055–1062 (2007)