# O Peer, Where Art Thou? Uncovering Remote Peering Interconnections at IXPs

Vasileios Giotsas, George Nomikos, Vasileios Kotronis, Pavlos Sermpezis, Petros Gigis, Lefteris Manassakis, Christoph Dietzel, Stavros Konstantaras, and Xenofontas Dimitropoulos

***Abstract*—Internet eXchange Points (IXPs) are Internet hubs that mainly provide the switching infrastructure to interconnect networks and exchange traffic. While the initial goal of IXPs was to bring together networks residing in the same city or country, and thus keep *local traffic local*, this model is gradually shifting. Many networks connect to IXPs without having physical presence at their switching infrastructure. This practice, called *Remote Peering*, is changing the Internet topology and economy, and has become the subject of a contentious debate within the network operators' community. However, despite the increasing attention it attracts, the understanding of the characteristics and impact of remote peering is limited. In this work, we introduce and validate a heuristic methodology for discovering remote peers at IXPs. We (i) identify critical remote peering inference challenges, (ii) infer remote peers with high accuracy (>97%) and coverage (94%) per IXP, and (iii) characterize different aspects of the remote peering ecosystem by applying our methodology to 30 large IXPs. We observe that remote peering is a significantly common practice in all the studied IXPs; for the largest IXPs, remote peers account for 40% of their member base. We also show that today, IXP growth is mainly driven by remote peering, which contributes two times more than local peering.**

***Index Terms*—Communications technology, communication systems, communication networks, computer networks, Internet, IP networks, metropolitan area networks, Internet topology, telecommunications, telecommunication network topology.**

Manuscript received November 25, 2019; revised July 26, 2020; accepted August 19, 2020; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor M. Schapira. Date of publication October 23, 2020; date of current version February 17, 2021. This work was supported in part by the Lancaster Security Institute EC H2020 CONCORDIA under Grant 830927 for Lancaster University, in part by RAVEN under Grant ERC 875671 for ICS FORTH, and in part by Greece and the European Union (European Social Fund-ESF) through the Operational Programme Human Resources Development, Education and Lifelong Learning in the context of the project "Reinforcement of Postdoctoral Researchers-2nd Cycle" under Grant MIS-5033021, implemented by the State Scholarships Foundation (IKY) for Aristotle University. A preliminary version of this article appeared in the Proceedings of the ACM Internet Measurement Conference (IMC) 2018. *(Corresponding author: Vasileios Giotsas.)*

Vasileios Giotsas is with the School of Computing and Communications (SCC), Lancaster University, Lancaster LA1 4YW, U.K. (e-mail: v.giotsas@lancaster.ac.uk).

George Nomikos is with FORTH, 700 13 Heraklion, Greece, and also with the School of Computing and Communications (SCC), Lancaster University, Lancaster LA1 4YW, U.K.

Vasileios Kotronis and Lefteris Manassakis are with FORTH, 700 13 Heraklion, Greece.

Pavlos Sermpez is with the Department of Informatics, Aristotle University of Thessaloniki (AUTH), 541 24 Thessaloniki, Greece.

Petros Gigis is with the Department of Computer Science, University College London (UCL), London WC1E 6BT, U.K.

Christoph Dietzel is with the Products and Research Department, DE-CIX, 60314 Frankfurt, Germany, and also with TU Berlin, 10623 Berlin, Germany.

Stavros Konstantaras is with AMS-IX, 1017 XN Amsterdam, The Netherlands.

Xenofontas Dimitropoulos is with FORTH, 700 13 Heraklion, Greece, and also with the Computer Science Department, University of Crete, 700 13 Heraklion, Greece.

Digital Object Identifier 10.1109/TNET.2020.3025945

## I. INTRODUCTION

INTERNET eXchange Points (IXPs) are crucial components of today's Internet ecosystem [2]–[5], that provide infrastructure for the direct interconnection (*peering*) of Autonomous Systems (ASes). Currently, there exist more than 700 IXPs around the world, with more than 11K member networks (i.e., *peers*); these correspond to approximately 15% of the total number of ASes [6]–[8]. The largest IXPs host more than 800 networks each [9], [10], and handle aggregate traffic that peaks at or exceeds 6 Tbps [11], [12].

IXPs were originally created to locally interconnect ASes at layer-2 (L2), and *keep local traffic local* [13]. Under this model, networks peer at IXPs to *directly connect* with each other and avoid connections through third parties, and thus reduce costs, improve performance (*e.g.,* lower latency), and better control the exchanged traffic [14], [15]. However, the ever-increasing traffic flowing at the edge of the Internet, creates pressure for denser and more diverse peering that challenges the traditional IXP model. As a result, the IXP ecosystem is undergoing a fundamental shift in peering practices to respond to these requirements: networks may establish peering connections at IXPs from *remote* locations, to broaden the set of networks they reach within one AS-hop [16], [17], either over a (owned or rented) "long cable" or over *resellers* that provide ports on the IXP and L2 access through their own network [18], [19]. This practice contradicts the traditional view of IXPs as local hubs of direct peering and is commonly referred to as *Remote Peering* [15] by IXP operators, where "remote" denotes a distant connection to an IXP.

*Remote Peering (RP) is when a network peers at an IXP without being connected with the IXP at one or more of the facilities where the IXP has deployed its peering LAN.*

While RP has been actively advertised by IXPs, it has also fired up a heated debate within the operators' community [15], [20]. The *proponents* of RP highlight the benefits in connectivity and cost reduction for the IXP members, whereas the *opponents* emphasize on the risks and implications for network performance and resilience. Irrespective of which side in this debate one stands for, the reality is that RP is fundamentally changing the IXP peering landscape, with unclear effects on Internet economics and performance. Today we lack the tools and techniques to answer even simple questions, such as *"Which peers of an IXP are remote and which are local?"*. The answer to this question could significantly benefit Internet operations and drive routing policies and peering decisions (*e.g.,* eyeballs or content providers that seem local at an IXP may not be local). Such knowledge is therefore important both for IXP operators to understand the characteristics of their member base, and IXP members to perform *e.g.,* traffic engineering (TE) based on peering policies. Moreover, it enables researchers to explore different facets of RP ecosystems.

In this article, we propose a methodology to infer RP, and analyze its main characteristics. Our primary objective is to enable transparency, a property which is desired by all stakeholders, regardless of which side they pick in the RP debate. We first provide the necessary background on this debate in in Section II, as well as related work in Section III. After presenting our measurement datasets (Section IV), we make the following contributions:

**Identify inference challenges (Section V).** We first identify the difficulties of inferring RP, by collecting and analyzing a best-effort validation dataset of remote/local peers in 14 large IXPs. We show that inference based exclusively on latency measurements, as proposed by Castro *et al.* [21], is not capable of accurately inferring RP at scale.

**Infer remote peers (Section VI).** We design a novel methodology to infer whether a peer is remote or local to an IXP. Due to the involved complexity and challenges, we take into account multiple dimensions of peering, such as latency, colocation and IXP facility information, IXP port capacity and router connectivity, and combine them to achieve an accurate inference. Comparing our inferences against validation data shows that our approach achieves a 97% accuracy and 94% coverage, while the corresponding percentages of the state-of-the-art [21] are 77% and 84%, respectively.

**Characterize remote peering (Section VII).** We apply our methodology to 30 large IXPs, and analyze characteristics of RP. While an extensive evaluation of RP characteristics and implications is outside the scope of this work, we consider use cases that exhibit the applicability of our inference approach. We find that RP is prevalent today, with 28% of the peering interfaces being remote. Our results also show that today, IXP growth is mainly driven by remote peering, which contributes *two times more* than local peering with respect to the number of new IXP members. We also compare the end-to-end performance of remote IXP peering against full and partial layer-3 transit. Our results indicate that in terms of latency and jitter layer-2 remote peering offers a good tradeoff between QoS-optimized layer-3 WANs for partial transit and traditional BGP transit services.

Finally, in Section VIII, we present our new portal, a web-based remote IXP peering observatory [22] to visualize and make publicly available our inferences.

## II. Background

### A. Remote Peering

**Peering at IXPs.** ASes connect and exchange traffic (*i.e., peer*) with each other via bi- or multi-lateral setups at IXPs, which operate L2 switching platforms. Typically, ASes become *members* of an IXP by connecting to its infrastructure through their own router(s), colocated at the facility where the IXP has presence. This enables them to peer with other IXP members.

**Remote peering at IXPs.** Remote peering does not require physical presence of networks' routing equipment in the IXP fabric [23]. The connection is performed through: (i) *resellers* [24] of IXP ports that connect the remote peer's router(s) to the IXP switches, (ii) *L2 connections* ("long cables") to the IXP facility (with ports bought by the peer itself), either with privately owned cables or by using a carrier, and (iii) *IXP federations* [25], [26], *i.e.,* IXPs belonging to the same organization (like DE-CIX Frankfurt and DE-CIX New York), which are interconnected so that local peers of one IXP are remote to the other and vice versa.[1]

**The remote peering debate.** The increasing attention that remote peering is drawing has also given rise to a recent debate within the networking community [20], placing emphasis on the impact of remote peering on Internet routing and economics.

**Remote peering is good!** On the one hand, there are several advantages and new possibilities for *networks* peering remotely at an IXP:

- *Monetary savings.* CAPEX is reduced since there is no need for additional routing equipment, or colocation and installation fees [15], [27]. Remote peering can also be an option for offloading transit traffic [21].
- *Increased connectivity.* Networks can easily establish direct connections with more peers (*e.g.,* content providers present at remote IXPs), and have better control over traffic routed from / towards them.

For the *IXP*, remote peering leads to:

- *More members/customers.* IXPs can attract members which are present in different cities or countries, and thus, increase their market share. IXPs with many members are more visible and appealing to potential customers.
- *Reseller ecosystem.* The IXP can benefit from reseller organizations, which handle new IXP memberships at scale, and therefore the setup and billing of new members is simplified.

**Remote peering is bad!** On the other hand, some network and IXP operators claim that remote peering is a disservice to the Internet [15], [20]. IXPs have been originally created as peering hubs to keep "*local traffic local*" [13]. Changing this trend might lead to:

- *Degradation of performance.* Links over IXPs involving peers at distant locations from IXPs are expected to have larger latency (RTTs) than links between local peers. Hence, direct peering connections on IXPs might not necessarily lead to improved quality in communication. Additionally, resellers usually offer low capacity IXP ports (*e.g.,* 100Mbps; see Section VI-A.4), which can cause congestion [28].
- *Loss of resilience.* While a network might have separate L3 connections with its peers on an IXP, in the case of remote peering some of these connections might share a common port (*e.g.,* resellers sell fractions of the same physical IXP port to multiple remote peers). A single outage on this port can thus affect (a) multiple connections, and (b) networks hundreds or thousands of kilometers away from the IXP. As a result, neither traffic nor outages "stay local".

**Need for transparency.** While there is no consensus on whether remote peering is a good or bad practice, both its proponents and opponents acknowledge the necessity for understanding its characteristics. Network operators want to know which peers are local or remote, where they are located, and the implications on the communication (*e.g.,* latency, bandwidth, resilience) among peers. This knowledge is critical since it can guide traffic engineering and peering policies.

### B. Special Cases

**Wide-area IXPs.** Some IXPs are geographically distributed entities, possessing switching infrastructure in multiple

[1] The involved IXPs still use their own route servers and BGP communities and serve their own member base.

facilities in different metropolitan areas[2]/countries. We call such cases, where the IXP's L2 network spans large geographical areas, *wide-area* IXPs (WAIXP). An example of a WAIXP is NL-IX [29], spanning the European continent.[3] The members of a WAIXP are local peers, as long as they are directly patched to the switching infrastructure of at least one facility of the IXP (see Definition in Section I); otherwise (*i.e.,* if they are not colocated at any facility) they are remote. However, even if a peer is considered local at a WAIXP entity, it may be of interest to other peers to also have knowledge of its potential "remoteness" to certain metro areas where the WAIXP, but not the peer, is present, facility-wise. Note that such IXP setups can heavily complicate remote peering inferences (see Section V-B).

**Local & Indirect Peering.** There exist cases where a network has physical presence in the same metropolitan area and a nearby (or, even the same) facility to the IXP, but is connected *indirectly* to an IXP through a reseller network. This happens due to the fact that some networks require connectivity to the IXP via low bandwidth ports, which are not officially offered by the IXP itself. This can be achieved only by using the services (ports of fractional capacity) of an IXP reseller, even if the networks are colocated at the IXP's facilities (see also Section VI-A.4). This type of connection, to which we refer as "local-indirect peering", share most of the characteristics of remote peering, e.g., in terms of connectivity, costs, bandwidth, resilience; the only characteristic in which they may differ from purely remote connections, is the lower distance, and thus, latency. Inferring indirectness is a hard challenge due to the opaqueness of the intermediary (*i.e.,* the reseller); however, information such as assigned IXP port capacities can be helpful in this regard (see Section VI-A.4). Note that indirectness is orthogonal to locality; however, in practice, we see that most of the indirect peers are also remote, rather than local.

**Layer-3 Wide Area Networks** Partial transit offers an alternative option to remote peering over IXPs. Instead of buying layer-2 transit, an AS may buy layer-3 transit to reach only an IXP or a subset of ASes with which it wants to interconnect. Partial transit is often advertised as more cost effective than full transit, and with better Quality-of-Service (QoS) guarantees compared to public peering [30]. While partial transit is often offered by conventional ISPs, some partial transit providers follow principles of layer-2 IXPs in terms of how routes are exchanged between their customers, and the openness and transparency of their connectivity [31]. For example Hopus is a layer-3 peering broker which allows its customers to remove the Hopus ASN from their AS paths in order to achieve comparable path lengths to layer-2 peering [32]. However, layer-3 partial transit ISPs may self-declare IXPs as a marketing strategy to communicate a comparable cost effectiveness [33].

## III. Related Work

**IXP ecosystem.** Prior works on IXPs explore various aspects of the IXP ecosystem and show its impact on the Internet's hierarchical topology [2], [3], traffic exchange economics [4], [5], [34]–[36], and content delivery [13], [37], [38]. Specifically, Augustin *et al.* [3] employ traceroutes to detect IXPs and IXP peerings with high accuracy and coverage. Ager *et al.* [2] analyze traffic samples and examine the peering fabric of a large European IXP, showing the existence of a very diverse ecosystem in terms of business types, peering strategies, traffic exchanges, and geographic coverage. Lodhi *et al.* study open peering through game theory [35], and use a modeling and simulation-based approach to study peering relationships in transit providers [36]. In a practical context, Chatzis *et al.* [34] propel open IXPs and peering in the US to change the nation-specific economics of peering and interconnection. References [4] and [5] elaborate on the importance of the operational IXP ecosystem in the global Internet marketplace; among others, they hint at the increasing adoption of IXP port reselling and remote peering, without though delving in more detail. It is important to note that while these works study important IXP-related aspects, none of them differentiates between local and remote IXP members.

**Remote peering.** The role of remote peering (RP) in IXPs has only recently attracted the attention of research. Reference [39] discusses multilateral peering over IXPs at scale and shows that interconnection strategies, such as RP, and extensive colocation practices [40], create unexpected interdependencies among peering infrastructures. These interdependencies can lead to network disruptions [41] and/or outages [42]. In our methodology (in particular, in the steps related to facility detection), we build on concepts proposed by the measurement-driven facility-search methodology of [40]; however, [40] focuses more on pinpointing the exact facilities where an AS is present, rather than the local or remote nature of a peering connection.

Other works investigate the impact of RP on the topology or the performance of continental peering ecosystems. Gupta *et al.* [43] use BGP information and traceroutes to study ISP interconnectivity in Africa and discover circuitous paths between African ISPs; one of the reasons is that these ISPs must attain "backhaul" connectivity to large, distant IXPs in Europe, where they can achieve economies of scale. They do not explicitly delve into RP and use latency as the primary indicator for circuitous paths. Bian *et al.* [44] develops a methodology for detecting anycast prefixes based on passive measurements, yielding $\sim$90% accuracy. Using our Remote IXP Peering Observatory [22] they discovered that the false positives (unicast prefixes wrongly labeled as anycast prefixes) were due to RP practices. They estimate that in total, there are 19.2% of anycast prefixes potentially impacted by RP.

Closer to our paper is the work by Castro *et al.* [21], which explores the traffic offloading capabilities of RP and provides a simple RTT-based approach for inferring RP. Specifically, they study how to select ping vantage points and acquire robust RTT results for different IXPs, and how to define an appropriate "remoteness threshold" for RTTs. However, their approach does not take into account modern colocation and peering practices that can severely skew RTTs or lead to mis-inference. In this article, we show that RTT alone (as in [21]) is not sufficient to achieve accurate inference (see Section V). Instead, we combine RTT measurements with several other domain-specific design aspects of remote peering and achieve significantly larger accuracy and coverage levels, calculated using a substantial validation dataset. Our goal is to establish a general, thoroughly validated RP inference methodology and yield valuable insights on the global RP ecosystem.

[2] We consider as metropolitan area a disk with radius *50km*.

[3] While IXPs such as DE-CIX may have presence in multiple cities (e.g., Frankfurt, New York), they are not considered as WAIXPs, since they operate an independent/separate IXP at each city. In contrast, NL-IX is a sole IXP entity with a network distributed among multiple countries/cities.

## IV. Datasets & Measurements

### A. Active Measurement Sources

We use ping measurements to estimate the latency (RTT) between an IXP and its member ASes, and traceroute measurements to extract the IP-level paths traversing peering links.

**Pings.** We conduct ping measurements from a number of Vantage Points (VPs), namely *Looking Glasses (LGs)* and *RIPE Atlas probes (RA)*; the exact location of these VPs is known. Castro *et al.* [21] used the PCH LGs [7] that provided access to PCH border routers deployed in 22 IXPs. Unfortunately, PCH does not allow ping queries through their LGs anymore. Instead, using IXP websites, we compiled a list of 23 publicly accessible LGs, that provide direct interfaces inside the IXP networks, *e.g.,* to an IXP route server. To automate the querying of these LGs we use the Periscope platform [45].

We augment the set of the ping-enabled VPs through RA [46], a well-established global Internet measurement platform with more than 25,000 probes. To identify RA probes colocated with IXP infrastructure, we search for probes with source IPs in the address space of an IXP's peering LAN, and for probes which resolve to an ASN assigned to an IXP NOC.[4] We discovered 66 such RA probes.

Merging the available LG and RA VPs provides good coverage in the RIPE (29 IXPs) and APNIC (11 IXPs) regions. Only 6 IXPs are covered in the ARIN and LACNIC regions, and none under AFRINIC.

**Traceroutes.** We collect all the publicly available RA IPv4 traceroute paris measurements (*i.e.,* built-in and user-defined) [46]. In total, we study 3.15 billion traceroute paths towards $600K$ IPs, probed between Jan. 2017 and Mar. 2018. We use the collected traceroute paths to extract IP-level IXP crossings (see Section IV-C and steps 3, 4 of Section VI-B), as well as private connections between ASes over facilities (see step 5 of Section VI-B).

### B. IXP Peering LANs and Ports

Our methodology combines multiple sources of IXP-related information with the measurements of Section IV-A. The information is collected from publicly available databases, including IXP databases (e.g., PeeringDB) and IXP websites that provide machine-readable membership information.

**IXPs, members, and interfaces.** To identify traceroute hops that traverse IXPs, and feed our methodology with IXP-related information, we combine multiple sources to build an up-to-date list of *IXPs*, their *members*, and the *associated IXP interfaces* (*i.e.,* IP addresses belonging to IXP prefixes that are assigned to IXP member ASes). We retrieve the related IXP information directly from IXP websites by parsing the provided Euro-IX [47] `json` and/or `csv` machine-readable formats, and the publicly available databases of Hurricane Electric (HE) [6], PeeringDB (PDB) [8], and Packet Clearing House (PCH) [7].

To address cases of conflicting data, we consider IXP websites as the most reliable source of information since the data are directly provided by the IXP operators; in fact, while websites may share peering policy information with e.g., PeeringDB, they maintain their own IXP-related information, such as membership lists. We then rank the other IXP sources based on their fraction of conflicting entries compared to the website data (Table I). Consequently, we apply the following preference ordering to resolve conflicts: $IXP\ websites > HE > PDB > PCH$.

TABLE I

Overview of the IXP (IPv4) Dataset and Contribution of Each Data Source

| Source | IXP Prefixes | | | IXP Interfaces | | |
|---|---|---|---|---|---|---|
| | Total | Unique | Conflicts | Total | Unique | Conflicts |
| **Websites** | 42 | 4 | | 12409 | 24 | |
| **HE** | 429 | 51 | 1 (.010 %) | 29866 | 7659 | 80 (.27 %) |
| **PDB** | 638 | 187 | 1 (.005 %) | 22146 | 1162 | 62 (.28 %) |
| **PCH** | 467 | 129 | 1 (.007 %) | 5922 | 256 | 22 (.37 %) |
| **Total** | **731** | | | **31690** | | |

The final dataset includes $31,690$ IXP IP-to-AS mappings (*IXP interfaces*) and 731 IXP prefixes from 703 IXPs (Table I). Interestingly enough, the IXP prefixes and interfaces that are unique in the websites are quite few (4 and 24 respectively), since the other databases are usually populated with up-to-date entries. To the best of our knowledge, the collected dataset comprises the most complete list of IXPs, IXP prefixes, and IXP interfaces to-date.

**IXP port capacity.** We record the capacity of the peering ports allocated to each IXP member, using the `json/csv` datasets directly provided through the IXP websites, and the PDB records. For each IXP, we also compile the available port capacity options through the pricing section of its website [48]. As we explain in Section VI-A.4, knowing the port capacities allows us to distinguish IXP peers that obtain virtual ports through port resellers ("indirect" peers) from peers that obtain physical ports directly from the IXP ("direct" peers).

### C. Detecting IXP Crossings in Traceroutes

We process traceroute measurements (Section IV-A) and IXP information (Section IV-B) with `traIXroute` [49], [50] to identify paths that cross IXPs. We configure `traIXroute` to identify IXP crossings in a path, when (i) there exists a sub-path of three IPs (*i.e., IP triplet*) that contains an IXP IP in the middle of the triplet and this IXP IP belongs to the same AS as the $3^{rd}$ IP, (ii) the AS of the $1^{st}$ IP in the triplet is different, and (iii) these two ASes are members of the IXP (whose prefix the IXP IP of the triplet belongs to).

### D. Colocation Facilities

To infer the remoteness or locality of peers, we also use the location of the facilities where IXPs and their members are present. We first collect the facility list from PDB and *Inflect* [51], a database for Internet infrastructure services (whose data comes either directly from service providers or trusted third-party sources). For each facility we keep the geographical coordinates provided by PDB, which are independently verified through *Inflect* to filter-out spurious information [52]. Our dataset includes 656 IXPs which are associated with 1,078 facilities. The Inflect dataset allows us to correct the geographical information for 308 ($>$ 28%) of these facilities. Moreover, we extract information related to which facility each AS (i.e., IXP member) is present. About 60% of IXPs and ASes are present in a single facility. To alleviate possible incompleteness in PDB/Inflect data, we extend the

[4] Note that probes connected to the IXP members themselves are not useful for our methodology, since these members can be remote to the IXP, and thus may affect the RTT-based inference step biasing the ping measurements.

colocation dataset by *manually* extracting the facility list from the websites of the 50 IXPs with most AS members. IXP websites provide additional facility data for 48% of the IXPs, allowing us to compile an as complete as possible dataset for the most prominent IXPs.

**PDB *vs.* Websites.** We have encountered some discrepancies between PDB and IXP/facility websites. For example, the NL-IX website provides additional information on 17 (∼15%) of its data centers not present in PDB (incompleteness). However, for the CoreSite LA1 facility, PDB reports 108 ASes (∼43%) that are not listed in Coresite's list of locally deployed networks [53], indicating possible inaccuracies in PDB. Even in the face of such artifacts, the combination of the heuristics we apply in Section VI results to high accuracy/coverage.

TABLE II

ATTRIBUTES OF IXP PEERS AND REMOTE/LOCAL AND DIRECT/INDIRECT PEERING CHARACTERIZATION IN THE VALIDATION DATASET

| **Attributes** | | | **Characterization** | |
|---|---|---|---|---|
| **Colocation** | **Physical(P) / Virtual(V)** | **RTT Low(L) / High (H)** | **Local(L) / Remote(R)** | **Direct(D) / Indirect(I)** |
| ✓ | P | L | L | D |
| ✓ | V | L | L | I |
| ✓ | P | H | R | D |
| ✓ | V | H | R | I |
| X | P | L | R | D |
| X | P | H | R | D |
| X | V | L | R | I |
| X | V | H | R | I |

TABLE III

SUMMARY OF OUR CONTROL/TEST VALIDATION DATASETS

| | **IXP** | **#Facilities** | **#Total Peers** | **#Validated Peers** | **#Remote** | **#Local** |
|---|---|---|---|---|---|---|
| ***TEST*** | AMS-IX | 14 | 878 | 201 | 155 | 46 |
| | DE-CIX FRA | 28 | 795 | 270 | 236 | 34 |
| | MSK-IX | 14 | 428 | 98 | 76 | 22 |
| | France-IX PAR | 9 | 402 | 66 | 38 | 28 |
| | Any2 LA | 2 | 299 | 59 | 52 | 7 |
| | Seattle IX | 11 | 296 | 32 | 14 | 8 |
| | TOPIX | 7 | 102 | 66 | 61 | 5 |
| | LINX MAN | 3 | 99 | 20 | 12 | 8 |
| ***CONTROL*** | LINX LON | 15 | 770 | 183 | 144 | 39 |
| | TORIX | 7 | 260 | 57 | 53 | 4 |
| | DE-CIX NYC | 25 | 162 | 40 | 24 | 16 |
| | France IX MRS | 2 | 77 | 22 | 15 | 7 |
| | AMS-IX HK | 2 | 46 | 19 | 15 | 4 |
| | AMS-IX SF | 4 | 36 | 20 | 17 | 3 |
| | Total | 143 | 4650 | 1153 | 912 | 241 |

### *E. IXP Local/Remote Members for Validation*

Inferring remote peering accurately, requires thorough investigation of the challenges related to interconnectivity between IXPs and their members, as well as information to validate the peering inference itself. To this end, we collected and combined the following validation datasets.

*1) Remote Peers:* We first compiled two datasets used to validate true-positive/false-negative remote peering inferences.

**Ground-truth Connectivity:** First, we compiled a list of 912 remote peers at 14 different IXPs through ground-truth connectivity data by IXP conglomerates. For example, DE-CIX uses BGP Communities to annotate routes received over their GlobePEER platform [26], while France-IX publishes in their website members connected over its IXP partners, such as LUCIX, and TOP-IX [54]. We also collected published case studies by remote peering providers, and data reported by AS operators in their websites or directly to us through our Remote Peering Observatory portal [22].

**Router Geolocation:** We further used RIPE's IPMap [55] to geolocate the interfaces of the IXP members on routers connected to the IXP peering LAN, which we extract from the traceroutes described in Section IV-A. IPMap has been found to be over 98% accurate for country-level geolocation [56]. For increased accuracy, we run alias resolution using MIDAR [57] to group interfaces to routers, and we consider only alias groups with at least 3 interfaces that are all geolocated in the same city. When a router is geolocated in a country where the IXP has no facilities we consider the corresponding peer as remote (no possible colocation).

*2) Local Peers:* We also compiled two datasets to validate false-positive/true-negative inferences, as follows.

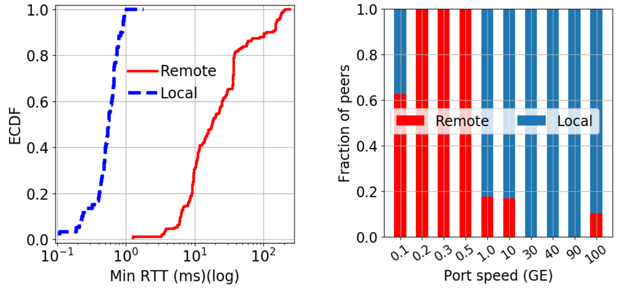
**BGP Looking Glasses**: We used BGP Looking Glass interfaces on border routers with known facility-level location that allow querying of the `show ip bgp summary` command to list the networks directly connected to the router. For routers located in a facility where an IXP is also present, if they are directly connected with the IXP's peering LAN, the `show ip bgp summary` command will list at least one next-hop IP in the IXP's prefix which means that the AS that operates the router is local to the IXP. This method allows us to collect 63 local IXP peers for 7 IXPs.

**IXP Resellers**: To provide remote connectivity, IXP resellers need to be local and directly connected to an IXP. To facilitate remote peering connectivity, most IXPs provide a detailed list of resellers for each of their location in their websites. We manually extract the list of resellers for 11 IXPs and map them to the corresponding ASNs, which allows us to compile an additional dataset of 178 local peers.

We also contacted IXP operators and asked for RTT measurements from within their infrastructure, as well as lists of their local and/or remote members. Unfortunately, none of the IXP operators could answer the question of which of their members are remotely connected via remote interconnection paradigms other than interconnections through IXP partners.

Instead, 6 of the IXPs provided RTT measurements and data on members connected through a reseller (on a "virtual" port). However, as explained in section II-B, in special cases an AS physically colocated with an IXP may prefer to connect through a reseller and not directly. By combining the reported reseller data and RTT measurements we found that 4̃0% of the virtual IXP peers have delay less than 10 ms. Therefore virtual connectivity does not reflect remoteness.

We list the different connection paradigms and attributes and corresponding characterization of local/remote or direct/indirect peers in Table II. We split our validation dataset into two subsets, *control* and *test*. We use the *control* subset in Section V to illuminate the remote peering ecosystem and investigate the challenges in the inference of remote peers. Based on these insights we develop our inference algorithm which we validate against the *test* subset in Section VI-C. In the test subset we include all IXPs with publicly accessible ping probes hosted in their infrastructure, since we use these probes to collect RTT measurements for our inferences. For the IXPs in our control dataset, we obtained one-time access to results from pings executed within the IXP infrastructure targeting the peering interfaces of all the IXP members. Both test and control validation datasets are contained in Table III.



**(a)** ECDF of minimum RTTs for remote and local peers in the control validation dataset. 40% of the remote peers have RTT less than than 10ms.

**(b)** The fraction of remote and local IXP members per port speed. Fractional ports (less than 1GE) are predominantly used for remote peering.

Fig. 1. Differences between local and remote IXP members in terms of port speeds and minimum latency from the IXP switches.

## V. RTT-Based Inference Challenges

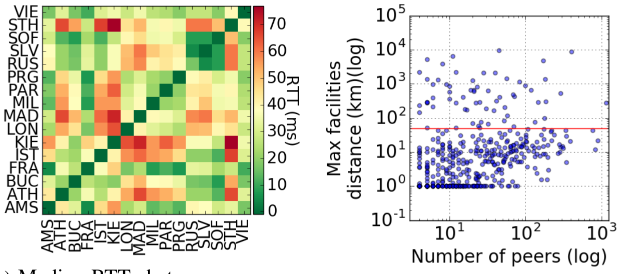
Here, we use the *control* subset of our validation dataset to investigate the challenges and limitations of inferring RP based exclusively on latency measurements (Section V-A), putting emphasis on the fairly common case of WAIXPs (Section V-B).

### A. RTT Is Not Enough

Based on the RTT datasets obtained from the IXPs, we apply the *TTL match* and *TTL switch* filters proposed in [21] to discard replies with TTL values less than the expected maximum (64 and 255 hops) that may indicate ping replies outside of the IXP subnet. We repeat the measurements every 20 minutes for two days, and we calculate the minimum RTT per IXP interface. As shown in Fig. 1a, RTT values above $2ms$ are a very strong indication of remote peers, with $99\%$ of the local peers having RTT values less than 1ms. This result is consistent with previous works that exhibited that a delay of 1ms corresponds roughly to a distance of 100 km ($2 \times 50$ km) [58], [59], approximating the coverage of a single metropolitan area (radius 50km). However, low RTT does not necessarily mean that a peer is local. Surprisingly, $40\%$ **of the remote peers in our control dataset are within 10ms**, which is the *"remoteness threshold"* used in [21].

### B. Wide-Area IXP Challenges

Conservative latency thresholds do not ensure the elimination of peers which are falsely identified as remote for *WAIXPs*. In fact, IXP members which are present in any of the facilities of such IXPs are local to the IXP but can be remote to the measurement VP, even if the VP is also hosted in one of the IXP's facilities. An indicative example is NET-IX, which has distributed its switching fabric in facilities across 18 different countries [60]. To understand the RTT characteristics among the different facilities of such a geographically distributed IXP, we obtained pairwise delay measurements between 16 of NET-IX's international sites. NET-IX measures the delay between its different facilities based on the Y.1731 Performance Monitoring standard [61], by sending precisely timestamped test packets across its MetroNID network demarcation points. The results are shown in Fig. 2a. For 87% of the facility pairs the median RTT is above $10ms$. Note that we also observe facilities in different countries with less than 10ms delay between them; for instance, Frankfurt (FRA) and Prague (PRA) have a $7ms$ delay. **Therefore, a remoteness RTT-threshold is not meaningful for WAIXPs.**



**(a)** Median RTTs between the facilities of the wide-area IXP NET-IX.

**(b)** Max. distance between IXP facilities, compared to the number of IXP members (source: PDB).

Fig. 2. Features of wide-area IXPs.

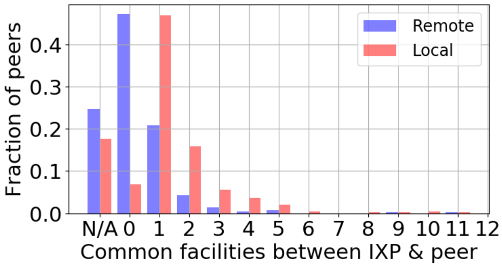
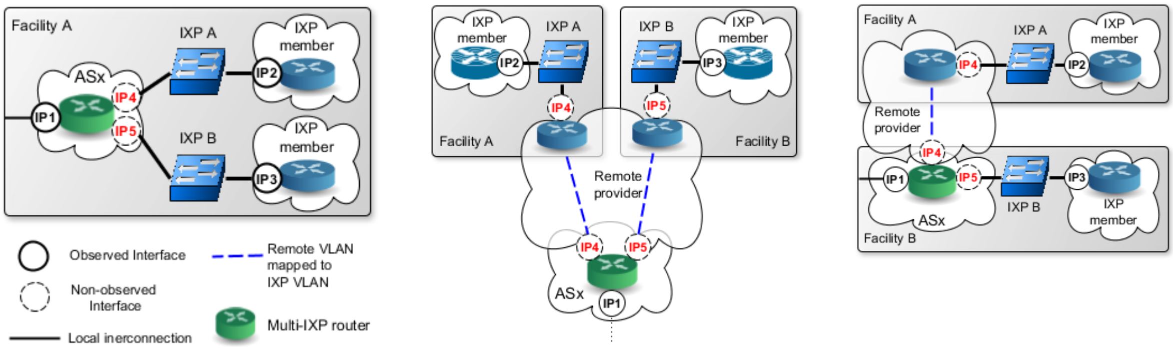


Fig. 3. Number of IXP facilities where local and remote peers in our control validation dataset are present.

Wide-area IXPs, such as NL-IX, run a unified L2 network spanning multiple facilities and metropolitan areas [29]. The IP address pool (from the peering LAN) that such an IXP assigns to its members is not location-specific; the IXP IP prefix(es) may in fact span several metro areas. **This makes remoteness inference on the level of the facility (or the metro area) extremely challenging,** requiring the combination of colocation data and latency measurements from one or more vantage points at the IXP facilities (see Section VI-B, Step 2).

Next, we quantify the popularity of the model of the WAIXPs. We use our colocation dataset compiled in Section IV-D, and we classify an IXP as wide-area if its switching fabric is deployed among multiple facilities, and at least two of them are in different metro areas. Since there can be different naming conventions used for the same city/metro area, we calculate the geodesic distance between each pair of IXP facilities, by applying Karney's method [62] on their geographical coordinates. We consider facilities more than $50km$ apart as located in different metro areas. For April 2018, we found that $64$ of the $446$ $(14.4\%)$ IXPs in PDB with at least two IXP members are wide-area, including $10$ of the $50$ $(20\%)$ largest IXPs in terms of the size of their IXP member list (Fig. 2). **Therefore, WAIXPs are fairly common and not just some exceptional cases.** Note that the infrastructure of some IXPs can be thousands of *kms* apart. For instance, NL-IX has facilities in London and Bucharest that are over 1,300km away from each other. This exacerbates the associated inference challenges.

The results of this section highlight that although RTT measurements have the potential to provide useful insights w.r.t. the peering approach employed by an IXP member, alone they are not adequate to accurately infer remote peers.



**(a)** Multiple local IXP peerings. **(b)** Multiple remote IXP peerings. **(c)** Local and remote IXP peerings.

Fig. 4. Different scenarios of *multi-IXP* routers, for which we may observe different traceroute paths where $IP_1$ precedes both IXP interfaces $IP_2$ and $IP_3$, indicating the presence of a multi-IXP router in $AS_x$.

A $10ms$-threshold is very conservative in the case of IXPs concentrated in a single metropolitan area, while it yields a large number of false positives in the case of WAIXPs.

## VI. Inference Methodology

To address the limitations of remote peering inference based exclusively on latency measurements, we introduce a “first-principles” [63] approach. We rely on domain-specific knowledge to identify technological (beyond latency) and economic aspects of peering connectivity (Section VI-A), and build upon these aspects to design a methodology for inferring remote and local peers (Section VI-B). We validate the proposed methodology in Section VI-C.

### A. Design Aspects

*1) Presence at Colocation Facilities:* To establish a direct connection to an IXP, an AS needs to deploy routing equipment in at least one colocation facility where the IXP has deployed switching equipment. *It is not possible for an AS to be a local peer of an IXP if they are not colocated in a facility*. As Fig. 3 shows, 96% of the local peers with facility data in our control validation dataset are present in at least one IXP facility, while 70% of the remote peers with known facilities do not have any common facility with the IXP. Hence, colocation provides a strong signal about the locality of an IXP member. However, the available colocation data for IXP members are incomplete and noisy. For example, in Fig. 3, there are no available data for 25% of the remote peers, while more than 20% of them claim to have presence in one IXP facility. To further investigate RP cases that claim colocation with the IXP, we contacted the IXP operators. Their feedback suggested that such cases are either an artifact of remote peers (not colocated with the IXP) adding the facility of their port reseller in their PDB record, or a consequence of the fact that peers (colocated with the IXP) prefer to connect through a port reseller in order to buy virtual ports of lower capacity at a discount price (see Section VI-A.4).

*2) Multi-IXP Routers:* An AS may connect to multiple IXPs through the same border router to reduce operational costs; we call such routers *multi-IXP routers*. The IP interfaces of a multi-IXP router might appear in different traceroute paths to be interconnected with different IXPs. We distinguish three cases where this is possible:

a) When multiple IXPs are present in the same facility, a colocated AS may connect directly to all of them using a single router (Figure 4a).
b) Remote peers may connect through the same provider (port reseller) to multiple remote IXPs where this provider has presence (Figure 4b).
c) An AS may connect with the same router to both local and remote IXPs, if it is e.g., colocated with one IXP and uses a reseller for another (Figure 4c).

*3) Private Connectivity:* Two networks colocated at the same IXP-hosting facility can interconnect with each other (*private peering*) without using the IXP infrastructure, *e.g.,* by directly connecting their routers. This might be a more economical solution in case they exchange large volumes of traffic [64]. Therefore, when an IXP member appears to be privately connected with several ASes which are colocated at the facility of the same IXP, this is a strong indication that this member is local to the IXP.

*4) Port Capacity:* IXPs offer to ASes connectivity to switch ports, whose capacity is typically between 1GE and 100GE [65]. To make port reselling an attractive service, resellers split their physical ports to multiple virtual ports (e.g., via sub-interfaces/VLANs) of lower capacity (rate-limiting), and offer them to remote peers at lower prices. *Fractional port capacities can be purchased only through resellers today*.[5] Thus, this information can indicate a network that peers remotely, via a reseller, at an IXP. Figure 1b shows the fraction of remote and local peers per port capacity in our control validation dataset. Port capacities below 1GE (the minimum capacity for physical ports offered by the corresponding IXPs), are predominantly used to establish remote peering, while port capacities above 10GE are almost exclusively allocated to local peers. Nonetheless, about 40% of the 1FE ports are used by local peers. These are either legacy peers that have not updated their port capacities, or local peers that opt to connect to the IXP through a re-seller for cost saving purposes. Similarly, 10% of the 100GE ports are used by remote peers that connect to the IXP through a layer-2 provider.

### B. Algorithm

We next describe our methodology for inferring remote peering, by combining RTT measurements with the four peering aspects discussed in Section VI-A. Step 1 (RTT measurement) generates RTT data, which are combined with facility

[5] In rare cases, some old IXP members are connected to physical ports of capacity less than the minimum offered today. This can be also due to stale entries in PDB.

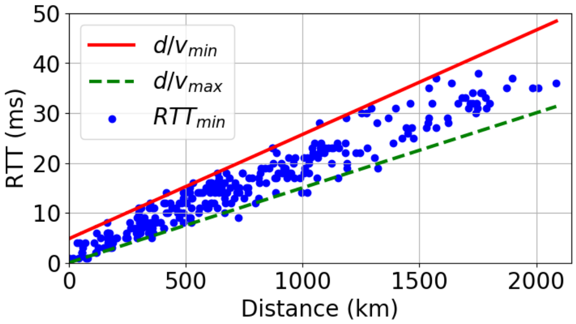


Fig. 5. Inter-facility RTT as a function of distance, based on Y.1731 Perf. Monitoring measurements from NL-IX and NET-IX.

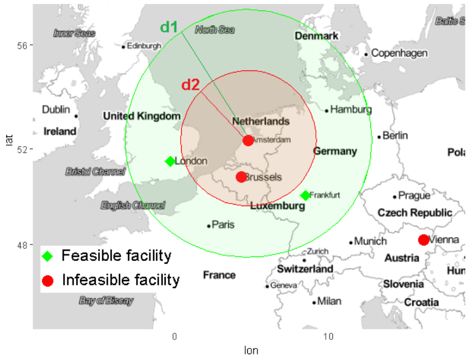


Fig. 6. Example of combining RTT measurements with IXP colocation data to infer local peers at geographically distributed IXPs.

colocation data in Step 2 (RTT+colocation) to accurately infer the majority of local/remote peers. Step 3 (multi-IXP routers) and Step 4 (port capacities and private connectivity) are based on inferences made in previous steps and employ heuristics to infer remoteness when RTT or colocation data are missing; Step 3 comes before Step 4 due to its higher accuracy. While an individual step may miss some cases for different reasons (e.g., incomplete colocation data or RTT outliers in Step 2), these cases can be captured by following steps.

*Step 1 (Ping RTT Measurements):* From every VP in an IXP (see Section IV-A), we execute ping measurements to every IXP IP interface of the IXP's members (see Section IV-B). To reduce the sensitivity of the results to network conditions, we repeat the measurements every two hours for two days, which results in 24 measurements in total for each {VP, IP interface} pair. Similarly to Section V, we apply the *TTL match* and *TTL switch* filters to discard measurements without consistent TTL values. Finally, for each responsive IP interface we store the minimum RTT value, $RTT_{min}$, to counter transient latency inflation artifacts [66].

*Step 2 (Colocation-Informed RTT Interpretation):* To infer local and remote peers, we analyze the collected $RTT_{min}$ values. Besides the colocation information of the IXPs and its members (see Section IV-D), the exact locations of the VPs are also known in all ping measurements. From the value of the $RTT_{min}$ we calculate a geographical area (circle or ring) around the VP location where the IP interface (and thus the router) of the IXP member can be located. The presence (or not) of a facility of the IXP in this area, denotes a local (or remote) peering, respectively.

More precisely, we first calculate the distance between the involved VPs and each of the IXP's facilities, as described in Section V. Then, from the observed $RTT_{min}$, we calculate the potential distance between the VP and the ping target (IP interface at a member's router). Katz-Bassett *et. al* [58] found that the end-to-end probe packet speed is at most $v_{max} = \frac{4}{9} \times c$, where $c$ is the speed of light. As shown in Fig. 5 (green/dashed curve), our dataset of facility-to-facility delays based on Y.1731 measurements obtained from NL-IX and NET-IX confirms this. Through data fitting, we also find an approximate lower bound (red/continuous curve in Fig. 5) for the speed $v_{min}(d) = \frac{d}{0.021 \cdot d? + 4.8}$, where $d$ is the distance. Based on these bounds,[6] we estimate that the ping target is within a distance range $D_{feasible} = [d_{min}, d_{max}]$ (green area in Fig. 6) from the VP, where $d_{min} = v_{min} \times RTT_{min}$ and $d_{max} = v_{max} \times RTT_{min}$. We call the facility that is located in $D_{feasible}$, a *feasible facility*.

Based on the estimated area defined by $D_{feasible}$ (see *e.g.*, Fig. 6), and the distances between the IXP facilities and the VP, we infer that the IXP member that owns the queried IP interface (ping target) is local or remote to the IXP, as follows:

1) ***Remote peer***: if (i) the IXP has no available feasible facility, or (ii) the IXP has at least one feasible facility, but the peer is not present at that facility.
2) ***Local peer***: if the IXP has at least one feasible facility, and the IXP member is also colocated in one of the feasible IXP facilities.
3) ***No inference***: if the IXP has at least one feasible facility, but the IXP member is *not* present at any feasible facility.

In the latter case, it is likely that our colocation dataset is incomplete w.r.t. the given peer. In this case we do not make an inference yet, but instead we leverage *multi-IXP router* and *private connectivity* information (see Section VI-A) as described in the following steps.

Combining RTT values with colocation information allows us to alleviate false positives caused by WAIXPs. Figure 6 shows an example of such a case, based on the topology of the NL-IX IXP. The IXP has distributed its peering fabric across multiple cities, including Amsterdam, Brussels, London, Frankfurt and Vienna. Our measurement VP is in an IXP facility in Amsterdam, from which we ping the IXP peering interfaces. Assume that for an interface $IP_x$ we measure an $RTT_{min}$ of $4ms$. Without taking into consideration the geographical footprint of the IXP's infrastructure we would infer the corresponding peer as remote assuming a "reasonable" (see Fig. 1a) $2ms$-threshold. Instead, we find that the IXP has two feasible facilities (London and Frankfurt) in the ring between $d_1 = 532km$ and $d_2 = 299km$ from the VP, as defined by our $v_{max}$ (green area) and $v_{min}$ (red area) bounds respectively, allowing us to infer as local the IXP members colocated at these facilities.

Similarly, we can avoid false negatives due to remote peers that are in close proximity to the IXP. For instance, for a peer located in Rotterdam connected remotely to the IXP's facility in Amsterdam ($57km$ distance) we will typically measure $RTT_{min} < 2ms$. By using the peer's collocation data we can correctly determine that, despite the low RTT, the peer is not local.

Optionally, by employing IXP colocation data, we can group the facilities of a WAIXP per metro area as {IXP, metro}. Afterwards, applying the colocation-informed RTT

[6] Out-of-bounds outliers do not impact the step's accuracy (see Table V).

interpretation for the metro tuples (having access to at least one vantage point in one of the IXP facilities), we can proceed to more fine-grained inferences and drill down on the exact peering setup of a local IXP member (which can be remote to some of the IXP facilities) as follows: {member, IXP, local} → {member, IXP, metro_1, local}, {member, IXP, metro_2, remote}, *etc.* While this does not affect the characterization of remoteness at the IXP level, it may be useful to WAIXP member operators.

*Step 3 (Multi-IXP Router Inference):* The previous steps may not be able to infer the peering type due to missing facility data or missing RTT values from unresponsive IXP interfaces. In such cases, we proceed to use the multi-IXP router feature (see Section VI-A.2), for inferring remoteness (or locality).

To identify multi-IXP routers we first collect traceroute paths from public RIPE Atlas measurements in the same period as our ping campaign (two days). We then extract the IP-level IXP crossings, as explained in Section IV-C, and we collect all sequences of hops $\{IP_x, IP_{x+1}^{IXP}\}$, where the interface $IP_{x+1}^{IXP}$ belongs to the address space of an IXP, and the interface $IP_x$ belongs to an AS that is a member of this IXP. For each AS that appears to peer at more than one IXP in different IXP crossings, we perform alias resolution on all its IP interfaces using MIDAR [57] to map these interfaces to routers.[7] For interfaces on the same router, we find the set of IXPs that appear as next hops in traceroute paths. If a router appears to have connections to more than one IXPs, we characterize it as a multi-IXP router.

For example, assume two sequences of IP hops, $\{IP_a$, $IP_{IXP1}\}$ and $\{IP_b, IP_{IXP2}\}$, where both $IP_a$ and $IP_b$ are owned by the same AS and are mapped to the same router $R$, and $IP_{IXP1}$ and $IP_{IXP2}$ belong to the peering LANs of $IXP1$ and $IXP2$, respectively. In this case, $R$ has layer-3 connectivity with both IXPs, and therefore we characterize $R$ as a multi-IXP router.

We then classify the multi-IXP routers in one of the categories described in Fig. 4, and infer each one based on colocation data from Section IV-D as follows:

1) ***Local multi-IXP router***: A multi-IXP router is local to all involved IXPs (Fig. 4a), if (i) the involved AS has been inferred as local peer –from previous steps– in at least one of the IXPs, and (ii) the involved IXPs have at least one common facility. Then *the AS is inferred as a local peer to all involved IXPs.*
2) ***Remote multi-IXP router***: A multi-IXP router is remote to all involved IXPs (Fig. 4b), if (i) the involved AS has been inferred as remote peer –from previous steps– in at least one of the IXPs (*e.g.,* $IXP_R$), and (ii) at least one of the following holds:
    a) all the involved IXPs have at least one common facility.
    b) the maximum distance between the facilities of any involved IXP and $IXP_R$, is smaller than the minimum possible distance $d_{min}$ between all the facilities of the involved AS and all the facilities where $IXP_R$ is present.

    Then *the AS is inferred as a remote peer to all involved IXPs.*
3) ***Hybrid multi-IXP router***: A multi-IXP router is local to a subset of the involved IXPs (Fig. 4c) and remote to another IXP subset, if (i) the involved AS has been inferred as local peer –from previous steps– in at least one of the IXPs (*e.g.,* $IXP_L$) of the local subset, and (ii) at least one of the following conditions is true for the remote subset:
    a) $IXP_L$ does not have any common facility with the other involved IXPs.
    b) the minimum distance between the facilities of $IXP_L$ and any other involved IXP, is larger than the maximum possible distance $d_{max}$ between all the (common) facilities where both the involved AS and $IXP_L$ are present.

    Then *the AS is inferred as a local peer to $IXP_L$ and remote peer to all other involved IXPs in the remote subset.*

To understand the intuition behind conditions $2(b)$ and $3(b)$, assume that $R_x \in AS_x$ is a multi-IXP router peering with two IXPs, $IXP_{ams}$ in Amsterdam, and $IXP_{lon}$ in London. The minimum distance between the facilities of the two IXPs is 300km, while the maximum distance is 360km. If from the first two steps we inferred that $AS_x$ is remote to $IXP_{ams}$, with $d_{min} = 500km$, then $R_x$ cannot be local to any facility of $IXP_{lon}$ (condition 2(b) holds). Similarly, if we inferred that $AS_x$ is local to $IXP_{ams}$ with $d_{max} = 50km$, then $R_x$ cannot be local to any facility of $IXP_{lon}$ (condition 3(b) holds).

*Step 4 (Finding Remote Peers via Port Capacities and Lack of Private Connectivity):* If Steps 1-3 fail to infer whether a peer is local or remote to an IXP, we combine data on port capacities with inference of private peering connectivity to determine the connection paradigm of this peer.

As discussed in Section VI-A.4, IXP ports of capacity lower than the minimum physical port capacity $C_{min}$ offered by the IXP, are only allocated to members that are connected to IXP through a reseller. Our analysis of the control validation dataset shows that resellers are predominantly used to enable remote peering. Hence, for each IXP member $AS_x$ that is not inferred yet as local/remote, we compare the port capacity $C_x$, reported either in the IXP website or the Inflect and PDB databases, to the $C_{min}$ value reported in the pricing section of the IXP's website. If $C_x < C_{min}$, we infer that *$AS_x$ is a remote peer* using a virtual port obtained through a reseller.

However, port capacities alone can lead to non-trivial false positives due to local peers that connect through port resellers to reduce cross-connect costs, or old IXP members connected to legacy physical ports of capacity less than the minimum offered today. To avoid such errors, we augment port capacity data with private connectivity of an IXP member and apply a "voting" scheme similar to the Constrained Facility Search (CFS) approach [40].

Let $\mathcal{F}_{IXP}$ be the set of feasible facilities for the IXP, $AS_x$ an IXP member identified based on the dataset of Section IV-B, and $\mathcal{I}_{IXP}$ the set of all IP interfaces of the multi-IXP routers identified in Step 3.

1) We parse all the collected traceroute paths, perform IP-to-AS mapping [69] and extract all the AS sequences over *private interconnections* (not over an IXP), *i.e.,* from a sequence $\{IP_i$,$IP_j\}$, where $IP_i$ belongs to $AS_i$ and $IP_j$ to $AS_j$ ($\neq AS_i$), we extract the sequence $\{AS_i$,$AS_j\}$. Let $I_{priv}$ be the set of all interfaces involved in such private AS-level interconnections.

[7] There are two available datasets: (i) one based on aliases resolved with MIDAR and `iffinder` [67], yielding the highest confidence aliases with very low false positives, and (ii) one also including aliases resolved with kapar [68], which significantly increases coverage at the cost of accuracy. We selected the first dataset to *favor accuracy over completeness*.

TABLE IV
VALIDATION SETS AND METRICS FOR RP INFERENCE

| | Name | Definition |
|---|---|---|
| Sets | $\mathcal{VD}_R$ | Remote Peers in Validation Dataset |
| | $\mathcal{VD}_L$ | Local Peers in Validation Dataset |
| | $\mathcal{VD}$ | $\mathcal{VD} = \mathcal{VD}_R \cup \mathcal{VD}_L$ |
| | $\mathcal{INF}_R$ | Inferred Remote Peers |
| | $\mathcal{INF}_L$ | Inferred Local Peers |
| | $\mathcal{INF}$ | $\mathcal{INF} = \mathcal{INF}_R \cup \mathcal{INF}_L$ |
| Metrics | COV | $\frac{\lvert\mathcal{INF}\cap\mathcal{VD}\rvert}{\lvert\mathcal{VD}\rvert}$ (Coverage) |
| | FPR | $\frac{\lvert\mathcal{INF}_R\cap\mathcal{VD}_L\rvert}{\lvert\mathcal{INF}\cap\mathcal{VD}_L\rvert}$ (False Positives rate) |
| | FNR | $\frac{\lvert\mathcal{INF}_L\cap\mathcal{VD}_R\rvert}{\lvert\mathcal{INF}\cap\mathcal{VD}_R\rvert}$ (False Negatives rate) |
| | PRE | $\frac{\lvert\mathcal{INF}_R\cap\mathcal{VD}_R\rvert}{\lvert\mathcal{INF}_R\cap\mathcal{VD}_R\rvert+\lvert\mathcal{INF}_R\cap\mathcal{VD}_L\rvert}$ (Precision) |
| | ACC | $\frac{\lvert\mathcal{INF}_R\cap\mathcal{VD}_R\rvert+\lvert\mathcal{INF}_L\cap\mathcal{VD}_L\rvert}{\lvert\mathcal{INF}\cap\mathcal{VD}\rvert}$ (Accuracy) |

TABLE V
VALIDATION OF DIFFERENT STEPS OF THE ALGORITHM

| **Methodology Steps** | **Feature** | **FPR** | **FNR** | **PRE** | **ACC** | **COV** |
|---|---|---|---|---|---|---|
| | $RTT_{min}$ [21] | 17.5% | 25.7% | 85% | 77% | 84% |
| Step 1+2: | $RTT_{min}$+Colo | 1.5% | 5% | 96.5% | 97% | 81% |
| Step 1-3: | Multi-IXP | 2% | 4.9% | 95% | 97.7% | 8% |
| Step 1-4: | Private Links | 4% | 9% | 92% | 94.3% | 4% |
| | **Combined** | **1.6%** | **5.2%** | **96.6%** | **97.2%** | **94%** |

2) We run alias resolution on the interfaces in $I_{IXP} \cup I_{priv}$, that belong to IXP members for which we have not made an inference yet. For each router $R_x$ (belonging to an $AS_x$) with at least one interface $i \in I_{IXP}$, we compile the set $\mathcal{N}_x$ of the (private) AS neighbors of $AS_x$.
3) Based on our AS-to-facility mapping from Section IV-D, we find the most common facilities $\mathcal{F}_{common}$ among the majority of the ASes in $\mathcal{N}_x$.

If $|\mathcal{F}_{IXP} \cap \mathcal{F}_{common}| = 1$, *i.e.,* only one facility of the IXP belongs to both sets, then *we infer $AS_x$ as a local peer to the $IXP$*. Otherwise, for peers with fractional IXP port capacities *we infer the peer as remote to the IXP*, The intuition behind this heuristic is that private interconnections are typically established within the same facility, as explained in VI-A.3. Nonetheless, we do not require all the private AS neighbors to be present in $\mathcal{F}_{common}$ because tethered private interconnections across facilities –although less common– are still possible [40].

### C. Validation

We validate each step of our methodology independently by comparing inference results (see Section VII-A) against the *test* subset of the validation dataset (see Section IV-E). The validation metrics we use and the sets that we consider are defined in Table IV. Note that concerning validation data it holds that $\mathcal{VD}_R \cap \mathcal{VD}_L = \emptyset$ (on the interface level), and in the metrics we do not take into account inferences for peers with no validation data (*i.e., $\mathcal{INF} - \mathcal{VD} = \emptyset$*). Table V shows the validation results for all IXPs in the test dataset, for different step combinations, as well as the entire algorithm.

**State-of-the-art.** As a baseline, we first validate the remote inference when using only $RTT_{min}$ (*step 1*), assuming a remoteness threshold of $10ms$ [21], to quantify the improvement versus the state of the art [21] achieved by our algorithm. $RTT_{min}$ yields a high $FPR$ due to mis-inferring local peers at WAIXPs as remote. We calculated that when excluding WAIXPs, the $FPR$ of the $RTT_{min}$ approach drops to 2%. At the same time, the $FNR$ is also high since many of the remote peers have $RTT_{min} < 10ms$, and remains at the same levels even when excluding the WAIXPs.

**Proposed methodology**. When combining $RTT_{min}$ with colocation data from Section IV-D (*steps 1+2*) we improve significantly all validation metrics; only the coverage metric has a small decrease, due to the fact that both latency and facility data are required. The false-negative inferences of $RTT_{min} + Colo$ are probably due to colocation data. For the next two steps we utilize traceroute data from Section IV-A. Specifically, the *Multi-IXP* step (*step 3*) also exhibits very high PRE and ACC. In our results, it contributes only about 8% additional inferences on top of steps 1-2, because we managed to collect extensive RTT and colocation data. Nonetheless, we found that it can contribute a coverage of almost 50% by excluding 11 of our ping VPs with $PRE$ and $COV$ still above 92%. The *Private Links* step (*step 4*) has the lowest ACC and PRE compared to the other steps and contributes about 4% additional inferences. Similar to the *Multi-IXP* step, when excluding the results from 11 of our ping VPs, the coverage of *Private Links* heuristic increases to 42% with $ACC$ and $PRE$ slightly below 85%. While this heuristic is used only as a "last-resort" step, it still outperforms vanilla RTT-based inference. When all the five steps are combined, they yield ~97% ACC and PRE, and cover 94% of the tested IXP interfaces.

## VII. INFERRING REMOTE PEERING IN THE WILD

Here, we apply our inference methodology on the 30 largest IXPs in our dataset, step by step (Section VII-A). Having inferred RP at IXPs, we investigate some relevant use cases. Indicatively, we focus on RP features in Section VII-B. We further study aspects of the evolution of the RP ecosystem over time (Section VII-C). Finally, we illuminate facility-level remoteness for two large WAIXPs (Section V-B).

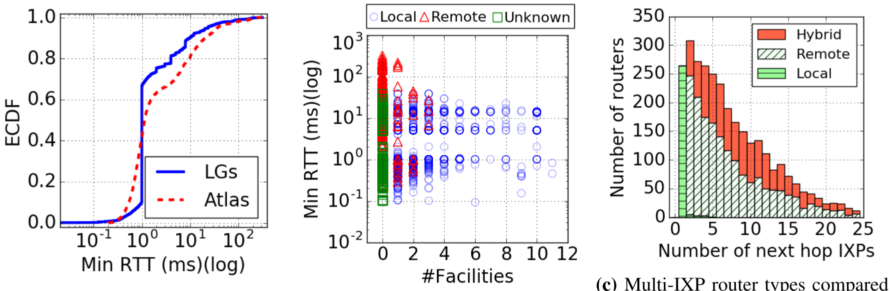
### A. Application of Step-Wise Inference

*Step 1:* We execute a ping measurement campaign between 7-9 Apr. 2018 from each LG and Atlas VP, to the peering interfaces of the IXP that hosts the VP. LGs achieve high response rates due to being directly attached to the IXP peering LAN. In contrast, 50 of the 66 Atlas probes are colocated within an IXP facility, but are not inside the IXP's LAN. Therefore, pings from them to IXP LAN IP addresses are more likely to fail for various reasons [70]. 14 of the Atlas probes do not receive any ping response.

Figure 7a shows the $RTT_{min}$ distributions between VPs (LGs and Atlas probes) and IXP interfaces. 75% of the IXP interfaces are within $2ms$ from the respective VP. ***More than 20% of the interfaces have $\mathbf{RTT_{min} > 10ms}$, a 2-fold increase since 2014*** [21], [71].

However, we found Atlas probes with consistently inflated RTT values.[8] Such probes may be deployed in the IXP's management LAN which may not be in the IXP's facilities,

[8] Atlas probes can yield measurement errors [66]; in our campaign, we account for non-persistent inflation by considering minimum RTTs over time.

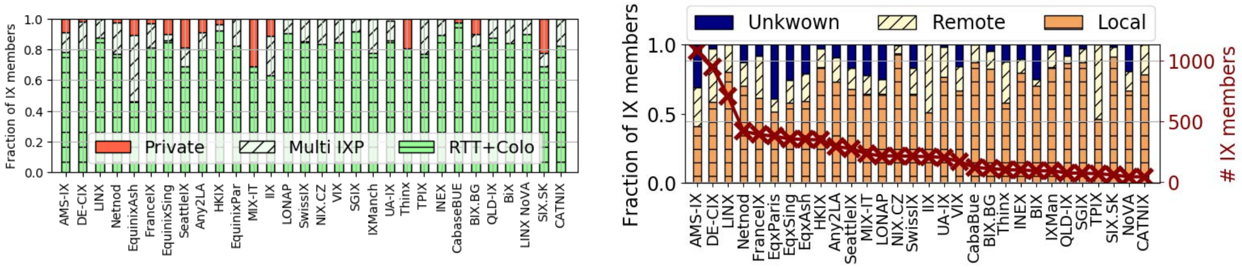


**(a)** ECDF of the min. RTT for each responsive IXP peering interface.

**(b)** $RTT_{min}$ for each IXP interface vs. number of feasible facilities.

**(c)** Multi-IXP router types compared to number of next-hop IXPs.

Fig. 7. Measurement results for RTTs, feasible facilities and multi-IXP routers.



**(a)** Contribution of each inference step per IXP.

**(b)** Inferences per IXP.

Fig. 8. Inference results for the 30 largest IXPs with LG/Atlas VPs.

but still abide to the *TTL match* filter (see Section V) which is set to $TTL_{max} - 1$ for Atlas probes. Thus, we discard probes that have $RTT_{min} \geq 1ms$ between the probe and the IXP's route server. This filter removes another 21 Atlas probes from the set of usable VPs. Also, note that a large number of minimum RTTs obtained from LGs are exactly $1ms$, which happens because many LGs round up the RTT value to the nearest integer. For such LGs we calculate the $d_{min}$ distance between the IXP interface and the VP assuming $RTT'_{min} = RTT_{min} - 1$, and we use the rounded-up $RTT_{min}$ to calculate the corresponding $d_{max}$ distance.

*Step 2:* We calculate the feasible IXP and AS facilities for each peering interface, based on the measured $RTT_{min}$, and infer the interfaces as local, remote or unknown, based on the combined latency and colocation information. Figure 7b shows the $RTT_{min}$ for each IXP interface versus the number of feasible facilities. Each $(RTT_{min}, \#facilities)$ data point is tagged with its inferred peering type. ***94% of the remote interfaces have no feasible common facility with the IXP*** (which further validates the colocation "principle"), while for 6% we have at least one feasible facility. Drilling down on this 6%, 40% of the involved interfaces exhibit $RTT_{min} > 2ms$, indicating spurious colocation information. Moreover, 5% of them are in a facility within the same metro area as the IXP VP but not affiliated with the IXP.

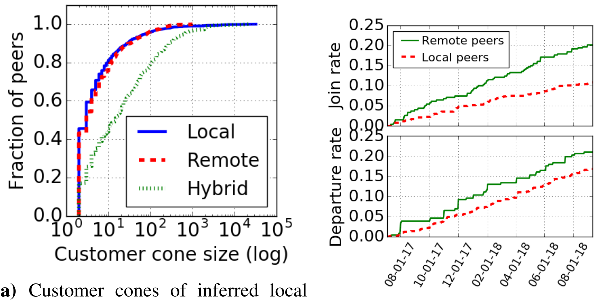
*Step 3:* For the *unknown* interfaces of Step 2, we investigate if they are part of multi-IXP routers. Figure 7c shows the number (per inferred type) of IXP routers compared to the number of IXPs with which they are connected (next-hop IXPs). Surprisingly, we find that 20% of the *unknown* interfaces and ***∼80% of the corresponding routers have multiple IXP connections, with 25% of them connecting to more than 10 IXPs***. This result highlights that the AS-level and IXP-level peering diversity of such IXP peers are misleading indicators of their resilience, since ***all of their interconnections depend on the same physical equipment*** (*i.e.,* the multi-IXP router). We further observe that cases of remote multi-IXP routers are more prevalent than hybrid ones.

*Step 4:* For the remaining unknown interfaces we infer locality or remoteness based on their IXP port capacities and private connectivity. As shown in Fig. 8a, we had to apply this heuristic only for 11 of the top 30 IXPs, because previous steps did not manage to successfully infer some of the IXP interfaces of these IXPs as remote or local.

**Overall.** In total, the contribution (in terms of fraction of inferences) of each step of the methodology is shown in Fig. 8a. Steps 1+2 $(RTT + colo)$ and 3 (multi-IXP routers) account for the majority of the inferences. Moreover, Fig. 8b shows the final inference results for the top 30 IXPs. Overall, ***we find 28% of all the IXP interfaces for which we made an inference to be remote. Also, for 90% of the IXPs, it holds that more than 10% of their members are remote peers.*** Finally, we find that for the two largest IXPs (DE-CIX and AMS-IX) almost 40% of their members are remote.

### *B. Features of Remote Peers*

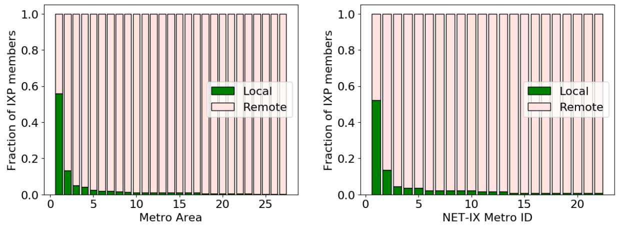
Having inferred remote and local peers per IXP, we proceed to investigate what are the features of remote peers and if/how they differentiate from local peers. We examine 3 features for each IXP member: (i) the size of its customer cone, as reported by CAIDA [72], (ii) its traffic levels and countries of presence as reported by PDB [8], and (iii) the user population it serves, as reported by APNIC [73]. We classify an IXP member network as follows: "remote" if it has only remote connections; "local" if it has only local connections; "hybrid" if it has both types (in the same or multiple IXPs). Out of 2959 total inferred AS peers in 30 IXPs, we find that 63.7% of these ASes are only local IXP members, 23.4% of the ASes are only remote IXP members, and 12.9% are hybrid, namely in some IXPs



**(a)** Customer cones of inferred local (blue), remote (red), hybrid (green) IXP members.

**(b)** The increase of remote peers is 2x faster compared to local peers.

Fig. 9. Features of all inferred IXP members.



**(a)** NL-IX. **(b)** NET-IX.

Fig. 10. Fraction of members of two WAIXPs that are local or remote to each metro area with affiliated IXP facilities. While both IXPs have distributed their infrastructure to over 20 metro areas, over half of their members are physically connected in single metro area, Amsterdam (NL) for NL-IX and Sofia (BG) for NET-IX.

they have local presence while in other IXPs they have remote presence.

In Fig. 9a we show the fractions of remote, local and hybrid IXP members with respect to the size of their customer cone. We observe that remote peers (red line) have quite similar patterns with the local ones (blue line). In fact, whether a network chooses to engage in local or remote peering (which is a matter of network design) at an IXP is not reflected on the size of its customer cone. This is probably due to the fact that both practices achieve similar Internet reachability to/from the local/remote peer's customers. Interestingly enough, member ASes that are local peers in some IXPs and remote in others tend to have one order of magnitude larger customer cones than the other cases. This is because hybrid IXP members are usually large ISPs that have diverse peering policies over large geographical areas, engaging both in local and remote peering depending on their business needs per market segment. Note that the insights pertaining to the customer cones of local, remote and hybrid peers are also reflected in the estimated user populations by APNIC (results omitted for brevity). Regarding the country distribution of the IXP members, we found that most local (13.86%) and hybrid (11.04%) peers are headquartered in GB, while PL seems to host the most remote peers (12.88%).

### C. Evolution of Remote Peering

To understand aspects of the evolution of RP over time, we collect (i) daily RTT measurements (pings) from available LG VPs in 5 IXPs (LINX, HKIX, LONAP, THINX and UAIX), (ii) PDB dumps, and (iii) Atlas traceroutes between 2017/07/04 - 2018/09/10, and we use them to infer remote and local peers across time. Based on this information, we can calculate aggregate growth (*i.e.,* a new member joins an IXP) and departure (*i.e.,* an old member leaves an IXP) rates *per peering type*. We observe that **the number of remote peers grows twice as fast as the number of local peers**, indicating that today, remote peers are the primary drivers of IXP growth (Fig. 9b). These results are confirmed by IXP annual reports from some of the largest IXPs (AMS-IX, DE-CIX, France-IX) [74]–[76], indicating that IXPs that already service the majority of local networks in their respective country-level peering ecosystems, seek to expand their market pool by attracting remote peers. However, remote peers also exhibit higher (+25%) departure rates than local ones; reseller customers do not commit substantial resources to establish their IXP connectivity (*e.g.,* routing equipment at the IXP), therefore it might be easier for them to terminate it. For the same time period we also found 18 cases of peers that switched from remote to local interconnections.

### D. Wide-Area IXPs: Locality Versus Metro-Level Remoteness

As described in Section II-B, wide-area IXPs (WAIXPs) are special peering setups. Peers that are remote to the WAIXP as an entity are remote to all its facilities; however, IXP-local peers may be local to only a subset of the available IXP facilities and remote to the rest. Our inference algorithm (see Step 2 of Section VI-B) allows fine-grained inference of such local/remote peering on a facility or metro area level. In Figures 10a and 10b, we show the fractions of IXP members of NL-IX and NET-IX (respectively) that are inferred as local/remote to different metro areas hosting affiliated IXP facilities. Interestingly enough, most of the IXP-local members are "concentrated" in a few of the available facilities in certain metro areas, in both IXP cases. While both IXPs have distributed their infrastructure across over 20 metro areas, over half of their members are physically connected in a single metro area; Amsterdam (NL) for NL-IX and Sofia (BG) for NET-IX. Each of the rest of the available metro areas attracts a minuscule portion of local peers. This is consistent with real data acquired from the two WAIXPS. **In summary, some WAIXPs can be approximated as present in a single metro area which attracts the majority of their local peers.**

### E. Performance Evaluation of Remote Interconnection Paradigms

As explained in Section II-B, an alternative to layer-2 remote peering are layer-3 WANs that offer potentially more flexible end-to-end QoS management and therefore improved performance in terms of latency, jitter and packet loss [77]. On the other hand, IXPs typically operate their switching fabric at a fraction of their backplane capacity, allowing them to avoid congestion even at times of sharp traffic peaks [78], while additional layer-3 hops can lead to inflated path lengths. To illuminate performance aspects of remote peering compared to conventional and partial ISP transit, we perform a campaign of Time-Sequence Latency Probe (TSLP) measurements [79]. TSLP involves contemporaneous frequent RTT measurements to the near-end and far-end interfaces of an interdomain interconnection. If the RTTs increase at the far-end but not at the near-end IP, it is a sign that the link is congested.

Figure 11 illustrates the setup of our measurement. For all three interconnection paradigms our strategy is to select measurement sources in ASes that are collocated at the

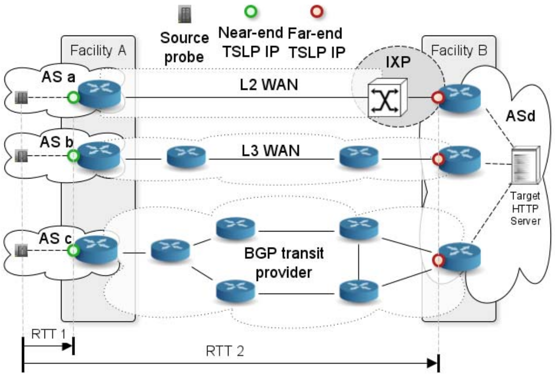


Fig. 11. Setup of Time-Sequence Latency Probe measurements to compare the performance of Layer-3 remote peering against a layer-3 peering WANs and conventional BGP transit.

same facility $A$, from where they establish their layer-2 or layer-3 connectivity. Every TSLP measurement targets the same destination IP, deployed in a metropolitan area remote from facility $A$. The border routers of the destination AS $AS_d$ are all colocated in the same facility (Facility $B$). Therefore all the path segments whose performance we evaluate have the same near-end and far-end facilities. Since two ASes that interconnect through a layer-3 provider may have multiple intermediary IP hops, we adapt TSLP to target the first and the last interfaces of the layer-3 transit segment, since we are interested in the performance of the entire transit path.

We focus our measurement campaign on Hopus, which is the most prominent provider of layer-3 peering. We select the destination IP to be in `AS39647`, which is one of the only two Hopus members not located in France [80]. `AS39647` interconnects from the NIKHEF Amsterdam facility to Hopus, two IXPs (AMS-IX and NL-ix) and a transit provider (Cogent). To avoid potential QoS policies that de-prioritize ICMP traffic, the destination IP is a non-anycasted public HTTP server. We select as measurement sources RIPE Atlas probes in Paris (FR) hosted in ASes that interconnect to one of Hopus, Cogent, AMS-IX or NL-ix. From each probe we issued TCP-based paris traceroutes to port 80 of the destination IP every 10 minutes between 16–26/06/2020. To accurately determine the location of the border routers we combine brmapit [81] to map the IPs of the border routers, and CFS [40] to pinpoint the facilities of those IPs. We found 5 source ASes for each interconnection paradigm (remote layer-2 IXP peering, Hopus partial transit, Cogent full transit) that all reach the destination IP from the "Telehouse - Paris 2" facility.

Figure 12 shows the distribution of our TSLP measurements per interconnection type. The L3 WAN of Hopus exhibits the highest median RTT (10.3 $ms$), but also the smallest standard deviation ($\sigma = 0.2\ ms$). In contrast, the transit network of Cogent has the lowest median RTT (9.2 $ms$), but the highest variability ($\sigma = 1.5\ ms$). Remote IXP peering offers a good trade-off with a median RTT of $9.5\ ms$ and $\sigma = 0.5\ ms$.

Our results indicate that both layer-2 remote IXP peering and QoS-optimized layer-3 WANs are not only more cost effective, but they can also offer performance benefits compared to traditional transit. However, a larger-scale measurement study would be required to generalize such results. Note that we conducted our measurements during lockdown measures in many countries to tackle the COVID-19 pandemic, which led to significant increase of Internet traffic volumes [78].

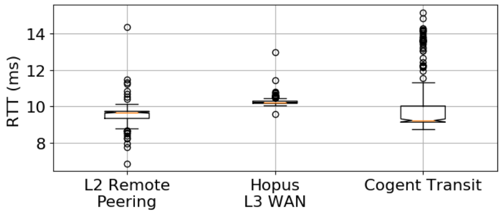


Fig. 12. Distribution of TSLP latency measurement results per interconnection type. Note the y-axis starts at 7 ms.

## VIII. Prototype and Portal

To automate our remote peering inference methodology and make our results publicly accessible to the community, we have implemented a web portal at [22], through which we publish monthly snapshots of our inferences, and visualize the geographical footprint of IXPs and their connected members. For each IXP the user can view the list of connected ASes, and the colocation facilities where the IXP has deployed its switching fabric. The user can query a specific IXP member to view the type of connection (local/remote), the minimum RTT measured by the most recent ping campaign, the port capacities and whether the IXP connection is established over a multi-IXP router. For remote interconnections the portal also displays the list of possible facilities from where the remote peers are likely connected. In addition to the graphical user interface, users can also query the inferences and raw data through a RESTful API to enable the automated consumption of the measurements. Finally, through the portal, IXP and AS operators are invited to contribute feedback, validation data, and access to additional measurement vantage points.

## IX. Conclusion

In this work, we introduce, validate, and apply a methodology that can infer remote and local peers at IXPs with high accuracy and coverage. Our methodology is built upon the observation that RP is not driven only by technical factors, but is actually a business decision guided by economic considerations. In particular, taking into account port capacities, colocation strategies, multi-IXP peerings as well as latencies and private connectivity practices, we achieve very high accuracy (97%) and coverage (94%) levels, outperforming the state-of-the-art by +20% and +10%, respectively. At the same time we reduce almost 10 times the false positive rates (and 5 times the false negative rates). The primary objective of this approach is to enable IXPs and existing or new potential IXP members to understand which peers of an IXP are *physically* local, allowing for better-informed peering and routing decisions. In our measurement-based study of 30 of the largest IXPs worldwide, we found that more than 90% of them have more than 10% of their members as remote peers. Strikingly, for large IXPs, this share may exceed 40%. The number of remote peers grows twice as fast compared to local peers, driving the IXP growth. The remote peers show similar patterns with local peers in terms of customer cones and user populations, indicating that remote peering is a widely adopted practice across networks.

**Future Work.** Knowing the locality or remoteness of IXP peering interconnections, a follow-up step is studying the volumes of traffic that flow over them, as well as the implications (performance, reliability, security) associated with routing this traffic over RP links. Moreover, by extending the methodology from pings to traceroutes, we can decouple it from the requirement of in-IXP vantage points and use the rich traceroute datasets available in projects such as RIPE Atlas [46] or Ark [82]. This will also enable going back further in time and performing decade-long longitudinal studies.

## References

[1] G. Nomikos *et al.*, "O peer, where art thou?: Uncovering remote peering interconnections at IXPs," in *Proc. Internet Meas. Conf.*, Oct. 2018, pp. 265–278.

[2] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a large European IXP," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 163–174, Sep. 2012.

[3] B. Augustin, B. Krishnamurthy, and W. Willinger, "IXPs: Mapped?" in *Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC)*, 2009, pp. 336–349.

[4] N. Chatzis, G. Smaragdakis, J. Böttger, T. Krenc, and A. Feldmann, "On the benefits of using a large IXP as an Internet vantage point," in *Proc. Conf. Internet Meas. Conf. (IMC)*, 2013, pp. 333–346.

[5] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "On the importance of Internet eXchange points for today's Internet ecosystem," 2013, *arXiv:1307.5264*. [Online]. Available: https://arxiv.org/abs/1307.5264

[6] Hurricane Electric. *Internet Exchange Report*. Accessed: Mar. 27, 2018. [Online]. Available: https://bgp.he.net/report/exchanges

[7] Packet Clearing House. *Internet Exchange Directory*. Accessed: Apr. 30, 2018. [Online]. Available: https://prefix.pch.net/applications/ixpdir/menu_download.php

[8] *PeeringDB*. Accessed: Apr. 30, 2018. [Online]. Available: https://www.peeringdb.com

[9] *AMS-IX Amsterdam: Connected Networks*. Accessed: May 13, 2018. [Online]. Available: https://ams-ix.net/connected_parties

[10] *DE-CIX Frankfurt Connected Networks*. Accessed: May 13, 2018. [Online]. Available: https://www.de-cix.net/en/locations/germany/frankfurt/connected-networks

[11] *AMS-IX Amsterdam: Traffic Statistics*. Accessed: May 13, 2018. [Online]. Available: https://ams-ix.net/technical/statistics

[12] *DE-CIX Frankfurt Traffic Statistics*. Accessed: May 13, 2018. [Online]. Available: https://www.de-cix.net/en/locations/germany/frankfurt/statistics

[13] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "There is more to IXPs than meets the eye," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 5, pp. 19–28, Oct. 2013, doi: 10.1145/2541468.2541473.

[14] A. Ahmed, Z. Shafiq, H. Bedi, and A. Khakpour, "Peering vs. Transit: Performance comparison of peering and transit interconnections," in *Proc. IEEE 25th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2017, pp. 1–10.

[15] W. B. Norton. (2012). *The Great Remote Peering Debate*. Accessed: May 13, 2018. [Online]. Available: https://goo.gl/yMrELB

[16] Y.-C. Chiu, B. Schlinker, A. B. Radhakrishnan, E. Katz-Bassett, and R. Govindan, "Are we one hop away from a better Internet?" in *Proc. ACM Conf. Internet Meas. Conf. (IMC)*, 2015, pp. 523–529.

[17] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, "10 lessons from 10 years of measuring and modeling the Internet's autonomous systems," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 9, pp. 1810–1821, Oct. 2011.

[18] *IX Reach Remote Peering Service*. Accessed: May 13, 2018. [Online]. Available: http://ixreach.com/services/remote-peering

[19] *RETN Remote Peering Service*. [Online]. Available: https://bit.ly/3hE2NLv

[20] *Remote Peering Panel Discussion*, 29th Euro-IX Forum, Krakow, Poland, Nov. 2016.

[21] I. Castro, J. C. Cardona, S. Gorinsky, and P. Francois, "Remote peering: More peering without Internet flattening," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2014, pp. 185–198.

[22] *Remote IXP Peering Observatory*. [Online]. Available: http://remote-ixp-peering.net

[23] A. Nipper. (Nov. 2016). Remote peering (with a look at Resellers as well). 29th Euro-IX Forum, Krakow, Poland. [Online]. Available: https://goo.gl/1ynm26

[24] S. Souquet. (Nov. 2016). France-IX reseller programme—Challenges and evolution after 4 years, 29th Euro-IX Forum, Krakow, Poland. Accessed: May 13, 2018. [Online]. Available: https://goo.gl/jRXs4b

[25] *AMS-IX EasyAccess Service*. Accessed: May 13, 2018. [Online]. Available: https://ams-ix.net/services-pricing/easyaccess

[26] *DE-CIX GlobePEER Remote Service*. Accessed: May 13, 2018. [Online]. Available: https://www.de-cix.net/en/de-cix-service-world/globepeer-remote

[27] W. B. Norton. (2013). *Understanding Remote Peering (Presentation)*. Accessed: May 13, 2018. [Online]. Available: https://goo.gl/3WruyV

[28] R. Fanou, F. Valera, and A. Dhamdhere, "Investigating the causes of congestion on the african IXP substrate," in *Proc. Internet Meas. Conf.*, Nov. 2017, pp. 57–63.

[29] *NL-IX: The Interconnect Exchange*. [Online]. Available: https://www.nl-ix.net

[30] W. B. Norton. *Partial-Route Internet Transit*. Accessed: Jul. 18, 2020. [Online]. Available: http://drpeering.net/HTML_IPP/chapters/ch11-07-Partial-Route-Internet-Transit/ch11-07-Partial-Route-Internet-Transit.html

[31] Hopus. *What is the Difference Between HOPUS and a IXP?* Accessed: Jul. 18, 2020. [Online]. Available: https://hopus.net/faq#tech

[32] A. Fenioux. *How to Put a Bird on a Docker Container on Arista*. FRNOG 33 Meeting. Accessed: Nov. 10, 2020. [Online]. Available: https://afenioux.fr/doc/presentations/FRnOG33-2019.pdf

[33] P. Smith. (Oct. 2016). Internet exchange point design. APNIC 42. [Online]. Available: https://bit.ly/2WXOHNa

[34] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "Quo vadis open-IX?" *ACM SIGCOMM CCR*, vol. 45, no. 1, pp. 12–18, 2015.

[35] A. Lodhi, A. Dhamdhere, and C. Dovrolis, "Open peering by Internet transit providers: Peer preference or peer pressure?" in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 2562–2570.

[36] A. Lodhi, N. Laoutaris, A. Dhamdhere, and C. Dovrolis, "Complexities in Internet peering: Understanding the 'black' in the 'black art,'" in *Proc. INFOCOM*, Apr. 2015, pp. 1778–1786.

[37] 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.*, vol. 48, no. 1, pp. 28–34, Jan. 2018, doi: 10.1145/3211852.3211857.

[38] V. Stocker, G. Smaragdakis, W. Lehr, and S. Bauer, "Content may be King, but (peering) location matters," in *Proc. ITS Eur.*, 2016.

[39] V. Giotsas, S. Zhou, M. Luckie, and K. Claffy, "Inferring multilateral peering," in *Proc. 9th ACM Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2013, pp. 247–258.

[40] V. Giotsas, G. Smaragdakis, B. Huffaker, M. Luckie, and K. Claffy, "Mapping peering interconnections to a facility," in *Proc. 11th ACM Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2015, pp. 1–13.

[41] A. Milolidakis, R. Fontugne, and X. Dimitropoulos, "Detecting network disruptions at colocation facilities," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 2161–2169.

[42] V. Giotsas, C. Dietzel, G. Smaragdakis, A. Feldmann, A. Berger, and E. Aben, "Detecting peering infrastructure outages in the wild," in *Proc. Conf. ACM Special Interest Group Data Commun.*, Aug. 2017, pp. 446–459.

[43] 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 *Proc. PAM*, 2014, pp. 204–213.

[44] R. Bian, S. Hao, H. Wang, A. Dhamdere, A. Dainotti, and C. Cotton, "Towards passive analysis of anycast in global routing: Unintended impact of remote peering," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 49, no. 3, pp. 18–25, Nov. 2019.

[45] V. Giotsas, A. Dhamdhere, and K. C. Claffy, "Periscope: Unifying looking glass querying," in *Proc. PAM*, 2016, pp. 177–189.

[46] *RIPE Atlas–Measurements*. Accessed: Oct. 11, 2020. [Online]. Available: https://atlas.ripe.net/

[47] IXPDB. *IXP Database*. Accessed: Oct. 11, 2020. [Online]. Available: https://www.ixpdb.net/en/ix-f/ixp-database

[48] J. Snijders, S. Abdel-Hafez, and M. Strong. *IXP Megabit Per Second Cost & Comparison*. Accessed: May 13, 2018. [Online]. Available: https://goo.gl/3nx1FJ

[49] *traIXroute–Source Code*. Accessed: Oct. 11, 2020. [Online]. Available: https://github.com/gnomikos/traIXroute

[50] G. Nomikos and X. Dimitropoulos, "traIXroute: Detecting IXPs in traceroute paths," in *Proc. PAM*, 2016, pp. 346–358.

[51] *Inflect: Find the Right Data Center*. Accessed: Oct. 11, 2020. [Online]. Available: https://inflect.com

[52] A. Nipper. (Nov. 2017). *PeeringDB Update, DENOG 9*. [Online]. Available: https://docs.peeringdb.com/presentation/20171123-DENOG9-nipper.pdf

[53] *Coresite Carrier List*. Accessed: Sep. 24, 2018. [Online]. Available: https://www.coresite.com/resources/resource-library/additional/carrier-list

[54] France-IX. *Interconnection With Other IXPs*. Accessed: May 13, 2018. [Online]. Available: https://www.franceix.net/en/solutions/interconnection/

[55] *RIPE IPmap*. Accessed: Oct. 11, 2020. [Online]. Available: https://ipmap.ripe.net/

[56] C. Iordanou, G. Smaragdakis, I. Poese, and N. Laoutaris, “Tracing cross border Web tracking,” in *Proc IMC ACM*, 2018, pp. 329–342.

[57] K. Keys, Y. Hyun, M. Luckie, and K. Claffy, “Internet-scale IPv4 alias resolution with MIDAR,” *IEEE/ACM Trans. Netw.*, vol. 21, no. 2, pp. 383–399, Apr. 2013.

[58] E. Katz-Bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, “Towards IP geolocation using delay and topology measurements,” in *Proc. 6th ACM SIGCOMM Internet Meas. (IMC)*, 2006, pp. 71–84.

[59] B. Trammell and M. Kühlewind, “Revisiting the privacy implications of two-way Internet latency data,” in *Proc. PAM*, 2018, pp. 73–84.

[60] (Apr. 2018). *NET-IX Network Map*. [Online]. Available: https://www.netix.net/network_map

[61] (Mar. 2011). *ITU-T Y.1731 Performance Monitoring In a Service Provider Network*. [Online]. Available: https://bit.ly/2CQa63R

[62] C. F. F. Karney, “Algorithms for geodesics,” *J. Geodesy*, vol. 87, no. 1, pp. 43–55, Jan. 2013.

[63] L. Li, D. Alderson, W. Willinger, and J. Doyle, “A first-principles approach to understanding the Internet’s router-level topology,” in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM)*, vol. 34, no. 4, 2004, pp. 3–14.

[64] W. Norton, *The 2014 Internet Peering Playbook: Connecting to Core Internet*. Palo Alto, CA, USA: DrPeering Press, 2014.

[65] *AMS-IX Amsterdam: Services and Pricing*. Accessed: May 13, 2018. [Online]. Available: https://ams-ix.net/services-pricing/pricing

[66] T. Holterbach, C. Pelsser, R. Bush, and L. Vanbever, “Quantifying interference between measurements on the RIPE atlas platform,” in *Proc. ACM Conf. Internet Meas. Conf. (IMC)*, 2015, pp. 437–443.

[67] CAIDA. *iffinder*. Accessed: Oct. 11, 2020. [Online]. Available: https://www.caida.org/tools/measurement/iffinder/

[68] CAIDA. *Kapar*. Accessed: Oct. 11, 2020. [Online]. Available: http://www.caida.org/tools/measurement/kapar

[69] CAIDA. *Routeviews prefix2as Dataset*. Accessed: Oct. 11, 2020. [Online]. Available: http://data.caida.org/datasets/routing/routeviews-prefix2as

[70] A. G. Mason and M. J. Newcomb, *Cisco Secure Internet Security Solutions*. Indianapolis, IN, USA: Cisco Press, 2001.

[71] I. Castro, J. C. Cardona, S. Gorinsky, and P. Francois. *Remote Peering Data*. Accessed: Nov. 25, 2019. [Online]. Available: https://svnext.networks.imdea.org/repos/RemotePeering

[72] *CAIDA AS Relationships*. Accessed: Oct. 11, 2020. [Online]. Available: http://www.caida.org/data/as-relationships

[73] APNIC. *IPv6 Measurement Campaign*. Accessed: Oct. 11, 2020. [Online]. Available: https://stats.labs.apnic.net/v6pop.

[74] AMS-IX. *AMS-IX 2016 Annual Report*. Accessed: Oct. 11, 2020. [Online]. Available: https://ams-ix.net/annual_report/2016

[75] DEC-IX. *DE-CIX Annual Report 2016*. Accessed: Oct. 11, 2020. [Online]. Available: https://goo.gl/qwCM23

[76] FRANCE-IX. *France-IX Annual Report 2017*. Accessed: Sep. 5, 2018. [Online]. Available: https://www.franceix.net/annual-report-2017

[77] T. Szigeti, C. Hattingh, R. Barton, and K. Briley, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd ed. Oxford, U.K.: Cisco Press Press, 2013, ch. 5.

[78] *Keeping the Internet Up and Running in Times of Crisis*, OECD, OECD Policy Responses to Coronavirus (COVID-19), Paris, France, May 2020.

[79] M. Luckie, A. Dhamdhere, D. Clark, B. Huffaker, and K. Claffy, “Challenges in inferring Internet interdomain congestion,” in *Proc. Conf. Internet Meas. Conf. (IMC)*, 2014, pp. 15–22.

[80] Hopus. *Member List*. Accessed: Jul. 18, 2020. [Online]. Available: https://hopus.net/members

[81] M. Luckie, A. Dhamdhere, B. Huffaker, D. Clark, and K. Claffy, “Bdrmap: Inference of borders between IP networks,” in *Proc. ACM Internet Meas. Conf. (IMC)*, 2016, pp. 381–396.

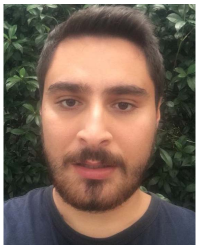
[82] UCSD CAIDA. *Archipelago (Ark) Measurement Infrastructure*. Accessed: Oct. 11, 2020. [Online]. Available: http://www.caida.org/projects/ark/

**Vasileios Giotsas** received the Ph.D. degree from University College London (UCL). He is currently a Lecturer with Lancaster University, where he leads the Networks Area Research of the Security Institute. His research interests include network measurements and the analysis of the routing systems.

**George Nomikos** received the B.Sc. degree in computer science from the University of Crete and the M.Sc. degree in communication systems and networks from the National and Kapodistrian University of Athens, Greece. He is currently pursuing the Ph.D. degree with Lancaster University. He is a Research and Systems Engineer with FORTH, Greece. His main research interests include Internet measurements and routing and network engineering.

**Vasileios Kotronis** received the Diploma degree in electrical and computer engineering from the National Technical University of Athens, Greece, and the Ph.D. degree in information technology and electrical engineering from ETH Zürich, Switzerland. He is currently a Post-Doctoral Researcher with FORTH, Greece. His main research interests include Internet routing, software defined networking, Internet measurements, and network security and engineering.

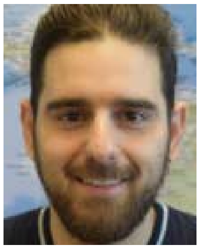
**Pavlos Sermpezis** received the Diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki (AUTH), Greece, and the Ph.D. degree in computer science and networks from EURECOM, Sophia Antipolis, France. He was a Post-Doctoral Researcher with FORTH, Greece. He is currently a Post-Doctoral Researcher with the Computer Science Department, AUTH. His main research interests include modeling and performance analysis for communication networks, network measurements, and data science.



**Petros Gigis** received the B.Sc. and M.Sc. degrees in computer science from the University of Crete, Greece. He is currently pursuing the Ph.D. degree in computer science with University College London, U.K. His main research interests include Internet routing, Internet measurements, software-defined networks, and cloud technologies.

**Lefteris Manassakis** received the B.Sc. degree from Greek Open University in 2009. He is currently pursuing the M.Sc. degree in network security with the Royal Holloway, University of London. He acquired more than 15 years of experience in IT industry before joining the Internet Security, Privacy, and Intelligence Research Group, Foundation for Research and Technology–Hellas, in 2016, as a Research Engineer. His research interests include Internet measurements, inter-domain routing, and network security.

**Christoph Dietzel** received the Ph.D. degree in computer science with a focus on Internet measurements/security, routing, and new networking technologies from Technische Universität Berlin. He is currently the Global Head of Products and Research with DE-CIX, responsible for product management, research and development, global network design, and project management. He is also affiliated with the Max Planck Institute for Informatics to combine practical IXP and computer network innovation with academic research. Prior to his current position, he was the Head of Research and Development with DE-CIX and responsible for several research initiatives, including numerous projects funded by the public sector.



**Stavros Konstantaras** received the B.Sc. degree in information technology engineering from the Alexander Technological Educational Institute of Thessaloniki and the M.Sc. degree in system and network engineering from the University of Amsterdam. He is currently a Network and Systems Engineer with Amsterdam Internet Exchange (AMS-IX). Before joining AMS-IX, he worked as an Internet Research Engineer at NLNet Labs and a Researcher at the University of Amsterdam. He has extensive operational and research experience on Internet routing security by leading the AMS-IX efforts to implement the recommended current practices and to deploy security toolchains.

**Xenofontas Dimitropoulos** received the Ph.D. degree from the Georgia Institute of Technology. He is currently an Associate Professor with the University of Crete and an Affiliated Researcher of the Foundation for Research and Technology–Hellas (FORTH), where he leads the Internet Security, Privacy, and Intelligence Research (INSPIRE) Group. His research interests include Internet measurements and Internet routing. He received three ERC grants.