Computer Networks 182 (2020) 107452

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Spoofed traffic inference at IXPs: Challenges, methods and analysis

Lucas Müller [a,b,*], Matthew Luckie [d], Bradley Huffaker [b,c], kc claffy [b,c], Marinho Barcellos [a,d]

[a] UFRGS, Brazil
[b] CAIDA, United States of America
[c] UC San Diego, United States of America
[d] University of Waikato, New Zealand

ARTICLE INFO

Keywords:
IP spoofing
Internet eXchange point
Denial-of-service
Network filtering

ABSTRACT

Ascertaining that a network will forward spoofed traffic usually requires an active probing vantage point in that network, effectively preventing a comprehensive view of this global Internet vulnerability. Recently, researchers have proposed using Internet Exchange Points (IXPs) as observatories to detect spoofed packets, by leveraging Autonomous System (AS) topology knowledge extracted from Border Gateway Protocol (BGP) data to infer which source addresses should legitimately appear across parts of the IXP switch fabric. We demonstrate that the existing literature does not capture several fundamental challenges to this approach, including noise in BGP data sources, heuristic AS relationship inference, and idiosyncrasies in IXP interconnectivity fabrics. We propose Spoofer-IX, a novel method to navigate these challenges, leveraging *customer cone* semantics of AS relationships to guide precise classification of inter-domain traffic as in-cone, out-of-cone (*spoofed*), unverifiable, bogon, and unassigned. We apply our method in three distinct periods to two IXPs, with 200+ and 1,600+ members each, and find an upper bound volume of out-of-cone traffic to be more than an order of magnitude less than the previous method inferred on the same data, revealing the practical importance of customer cone semantics in such analysis. We observed no significant improvement in deployment of Source Address Validation (SAV) in networks using the mid-size IXP between 2017 and 2019. In hopes that our methods and tools generalize to use by other IXPs who want to avoid use of their infrastructure for launching spoofed-source DoS attacks, we explore the feasibility of scaling the system to larger and more diverse IXP infrastructures. To promote this goal, and broad replicability of our results, we make the source code of Spoofer-IX publicly available.

1. Introduction

Networks that forward spoofed source Internet Protocol (IP) addresses in packets are a cybersecurity risk on the global Internet, because they enable attacks such as spoofed denial-of-service (DoS) attacks that are operationally infeasible to trace back to the actual source. Recognizing that lack of *source address validation* (SAV) is fundamentally an architectural limitation [1,2], the Internet Engineering Task Force (IETF) introduced best current practices recommending that networks block the forwarding of packets with spoofed source addresses [3,4]. Compliance with this practice faces misaligned incentives i.e., it protects the *rest* of the Internet from attacks being sourced from the network that must pay a non-trivial cost for deploying and accurately maintaining the filters. Thus, despite many attempts to improve SAV deployment, some of the most damaging DoS attacks in the Internet still leverage IP spoofing as a vector, setting new records each year for the volume of DoS traffic launched at even highly provisioned networks [5–8].

Identifying networks that do not filter spoofed packets is critical to global network infrastructure protection, because it provides a focus for remediation and policy interventions [9]. However, identification of these networks is challenging at Internet scale. The definitive method requires an active probing vantage point in each network being tested, to see if a spoofed packet successfully traverses the network [10,11]. Since there are approximately 700 K independently routed networks from almost 70 K autonomous systems (ASes) on the Internet in 2019 [12,13], this method has limited feasibility for a comprehensive assessment of Internet spoofing.

Broader visibility into the spoofing problem may lie in the capability to infer lack of SAV compliance from large, heavily aggregated Internet traffic data, such as traffic observable at Internet Exchange Points (IXPs). Most Autonomous Systems (ASes) connect to an IXP to exchange traffic between their customers, i.e., via peering relationships where neither AS pays the other for transit. For these ASes, legitimate source

* Corresponding author at: UFRGS, Brazil.
E-mail address: lfmuller@inf.ufrgs.br (L. Müller).

https://doi.org/10.1016/j.comnet.2020.107452
Received 20 January 2020; Received in revised form 23 June 2020; Accepted 27 July 2020
Available online 1 August 2020

addresses in packets will belong to direct or indirect customers of the AS sending the packets across the IXP fabric to their peers.

However, inferring SAV deployment at an IXP is remarkably challenging, far more so than has been captured in the literature, due to a combination of operational complexities that characterize today's interconnection ecosystem. First, determining which source addresses are valid in packets arriving at a given port of an IXP switch fabric is challenging, because there is no registry of which addresses networks should forward; in practice, we must heuristically infer valid source addresses. Second, while the original role of IXPs was to promote peering between ASes, networks now also use IXPs to obtain IP transit services from a provider [14], and we have found evidence of organizations joining their sibling network ASes across an IXP. For ASes offering transit across the IXP, and for sibling networks, it is infeasible to infer invalid source addresses from IXP traffic data — the set of valid addresses is potentially the entire address space. Third, while IXPs may be thought of as a single switching fabric, in practice we have observed in both medium and large IXPs complex services being offered both by the IXP and resellers, including remote peering, layer-2 transport, and virtualized segmenting of traffic into multiple Virtual Local Area Networks (VLANs). These interconnection practices occur below the network level and are thus not visible to the IP layer or in the Border Gateway Protocol (BGP). Besides, note that passive methods like ours are inherently unable to prove SAV is present, as they rely on unprotected networks actually forwarding spoofed packets.

Accurately inferring SAV deployment at an IXP requires understanding all these aspects and dealing with them the best way possible. In this paper, we describe a methodology that does so. One of our discoveries does not bode well for the ability to automate this method: identifying the myriad cases that explain patterns in traffic at a given IXP is largely manual in nature, and must be repeated at each IXP to accommodate IXP-specific architectural engineering and business decisions. However, we envisage its utility as part of an expert system suite of cybersecurity services or compliance practices of modern IXPs. To that extent, we apply this method to two IXPs in Brazil: IXP-M (medium) with over 200 members, and IXP-L (large), with over 1600 members. We use our methodology to classify and analyze packets in IXP-M considering two periods, 2017 and 2019. IXP-L is used to assess the feasibility of deploying our methodology to large switching fabric network infrastructures with multiple Colocation Facilities.

In our prior work [15], we presented the detailed development of Spoofer-IX, evaluating the methodology using traffic obtained from IXP-M. In this paper, we leverage data from IXP-L to confirm our insights and answer additional questions, by: (i) providing an analysis of the application of our methodology to a much larger IXP; (ii) conducting an in-depth analysis of the out-of-cone traffic nature; (iii) evaluating how consistent are filtering policies across AS members; (iv) characterizing the adoption of SAV over time.

This paper makes the following contributions:

(1) We provide a detailed analysis of methodological challenges for inferring spoofed packets at IXPs. We first review IP routing, addressing, and IXP concepts (Section 2), to clarify terminology, and we perform a comprehensive analysis of previous work that attempted to tackle this inference problem. We then analyze the methodological challenges and their implications for applying BGP-based SAV inference methods to modern IXP connectivity fabrics (Section 3).

(2) We develop a methodology to classify traffic flows for the purposes of accurately inferring spoofed traffic. We design and implement Spoofer-IX, a novel methodology to detect the transmission of spoofed traffic (which implies lack of source address validation) by AS members of IXPs (Section 4). Spoofer-IX addresses two fundamental issues overlooked in the existing literature [16]. First, Spoofer-IX considers the type of relationship between neighbors at an IXP when determining which source addresses are valid in IP packets crossing the IXP. Second, Spoofer-IX considers asymmetric routing and traffic engineering, by designing a prefix-level customer cone that includes addresses that may be valid source addresses for an AS to transit. The accuracy of this method depends on the quality of BGP data and AS relationship inferences, which we know to be imperfect [17]. However, our method is congruent with what network operators do when configuring static access control lists to deploy SAV [18–20].

(3) We use our methodology to classify and analyze packets at IXP-M considering two periods, two years apart. We apply our method to traffic and topology data (described in Section 5) from one of the largest IXPs in Brazil, IXP-M, with more than 200 member ASes using the IXP switching fabric. We report insights from the traffic classification conducted and our interaction with IXPs and network operators of their member ASes (Section 6). We investigate the impact of different filtering choices on inferred valid address space, and the likelihood of false negatives when classifying traffic according to different filtering choices. We also compare our method (Section 7) with a recently proposed method [16] that did not consider AS relationships in its inference of spoofed traffic, reporting that the majority of members at IXP-M sent spoofed packets, and demonstrate the inaccuracies of this approach. Indeed, this previous method inferred spoofed traffic coming from 62.3% of member ASes at IXP-M over a one-week period in May 2019, while our AS-relationship-aware method inferred spoofed traffic coming from fewer than 1 in 5 (18.7%) member ASes during our five-week observation period in May 2019, with no atypical traffic behavior associated with spoofed attacks, e.g., flooding, amplification (Section 8). At IXP-M, we observed no significant increase in the level of SAV deployment in attached networks when comparing 2017 and 2019 (Section 9).

(4) We discuss the deployment of Spoofer-IX to distinct networks. We partnered with IXP-L to assess the scalability of the Spoofer-IX method. We discuss (Section 10) how to scale the analysis by observing traffic per switch, and show the traffic classification results obtained in collaboration with three Colocation Facilities that constitute part of this large IXP. We also consider how networks could independently adopt our method to detect and filter spoofed traffic.

(5) We describe and publish our code to promote further work. Commercial and privacy sensitivities prevent sharing of traffic data that would enable directly reproducibility of much work in the field of Internet security. But in the interest of *replicability*, we publicly release our code [21] so that other researchers and IXPs can use it to improve our collective ability to measure and expand deployment of SAV filtering. We describe the set of tools we developed as part of Spoofer-IX (Section 4), which enables data extraction from switching fabrics, as well as traffic classification and analysis. All information regarding the datasets, setup, and software dependencies are publicly available in our project repository.

(6) We find evidence that epistemological and cross-validation challenges remain. We conclude our paper by summarizing the lessons learned (Section 12), including that we believe further work is required to understand the degree to which IXPs can be used as a lens into SAV deployment, and why we think such work is important to future cybersecurity efforts. Our conclusions highlight the persistent tension between the need for reproducibility of methods and results [22,23], and the opacity characteristic of commercial infrastructure.

2. Background and related work

2.1. Source address validation

The Internet architecture provides no explicit mechanism to prevent packets with forged headers from traversing the network. This vulnerability allows IP spoofing attacks, i.e., when hosts send IP packets using fake source addresses that cannot feasibly be traced back. To reduce the incidence of this type of attack, network operators can configure their routers to identify and drop (not forward) spoofed packets. Such filtering is well-specified and a standardized IETF best

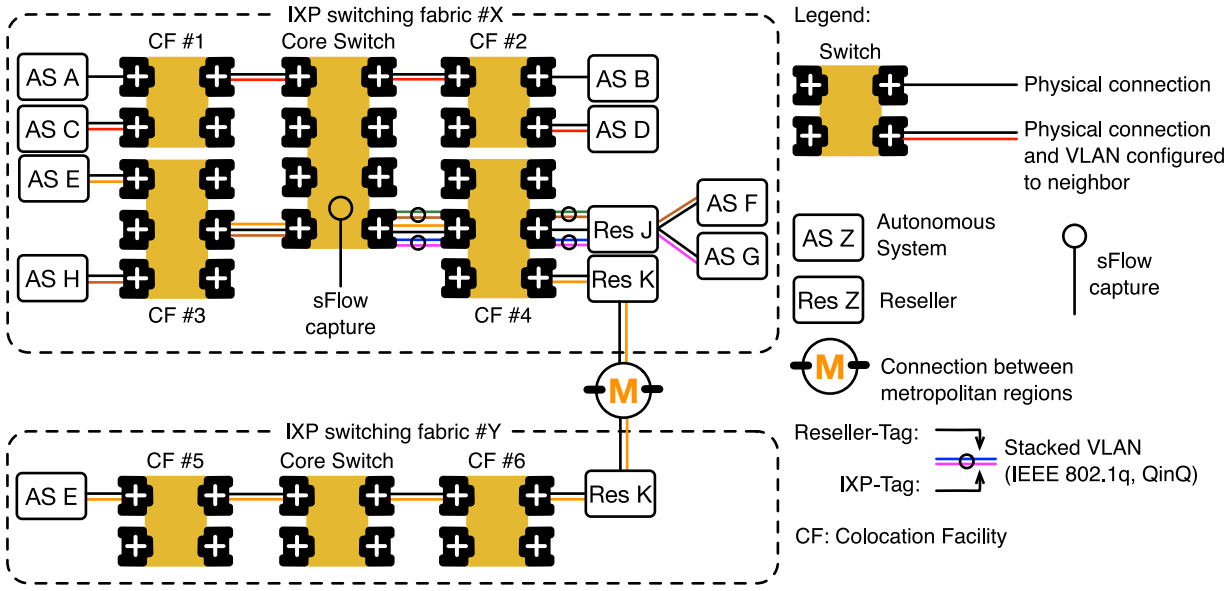


Fig. 1. Illustration of the architecture of modern IXPs. Modern IXPs typically construct a switching fabric using a core switch that interconnects other switches located in remote colocation facilities. ASes typically connect to a switch located in a colocation facility, and can form bilateral peering relationships with neighbors. These ASes may request a VLAN to isolate their traffic from other members at the IXP. Resellers can provide services such as remote peering and layer-2 transport.

current practice [3], frequently referred to as Source Address Validation (SAV) [24]. Network operators often implement SAV by using *ingress filters* in routers, which drop packets with source addresses outside the locally valid address space before they enter the global Internet.

2.2. Address space fundamentals

For the purposes of this study, we distinguish three main categories of IP address space: Bogon, Unassigned, and Routed. *Bogon* addresses are reserved by the IETF [25,26] for specific uses such as private networks and loopback interfaces; they do not uniquely identify any host, and should not be routed on the Internet. *Unassigned* addresses [27,28] have not been assigned by an Internet registry to an AS and should not be used or routed by anyone. *Routed* addresses have been assigned to some AS, and are thus potentially valid source addresses in inter-domain traffic.

2.3. IXPs as observatories

IXPs are attractive vantage points to observe signals of SAV deployment, as hundreds of ASes may be present at a single logical location. The IXP operator assigns each member a unique IP address from a prefix controlled by the operator, which the member assigns to their router interface connected to the IXP, and uses to establish BGP routing with other members. When a member AS's router transmits a packet across the Ethernet switching fabric, the source and destination media access control (MAC) addresses in the Ethernet frame uniquely identify the AS pair exchanging the packet, and its direction.

Fig. 1 illustrates the architecture of many modern IXPs [19,29–34]. It depicts the complexity of the existing components of the two IXPs, in which we apply our method, IXP-M and IXP-L. The figure contains two separate IXPs and their switching fabrics #X and #Y, with a core switch for each IXP. While some IXPs may consist of a single core switch where participants interconnect, operators achieve the scale of modern large IXPs by placing switches at distinct physical colocation facilities, any of which can serve as an IXP attachment point. The figure shows that the switches are adjacent, but in practice colocation facilities are usually in different buildings. IXP operators often use sFlow [35] or NetFlow [36] to collect traffic flow statistics. A comprehensive view of all traffic from all services at the IXP would require flow data captured from all switches in the switching fabric, as traffic between participants at a single colocation facility will not travel to the core switch.

Participants can exchange traffic directly across the switching fabric in a bilateral session. In Fig. 1, ASes A and B exchange traffic directly. However, modern IXPs often use VLANs to provide logical isolation between different types of interconnection [37,38]. For example, an IXP may provide a route server, but only offer that route server on a specific VLAN. Similarly, traffic between two participants may be sufficiently sensitive or high volume that members request a VLAN from the IXP to isolate their communications [39–41]. In Fig. 1, ASes C and D exchange traffic in their own isolated VLAN.

To foster IXP growth and enable more networks to interconnect, IXPs have supported resellers, which provide value-added services at an IXP, such as remote peering and layer-2 transport [42–45]. A reseller provides remote peering services so that an AS that is not physically present at a colocation facility can still reach other members at the IXP, without the AS incurring colocation facility fees or port charges from the IXP operator. These resellers require some cooperation with the IXP, e.g., [46,47]. The IXP assigns the remote peers any VLAN tags they require to participate at the exchange as local members do.

An IXP may use different technical approaches to support remote peering providers [34,42,43]. A reseller can bridge Ethernet networks so that the MAC address of the customer router's interface will uniquely identify the origin of traffic in the peering fabric. A second approach is for a reseller to push a tag (reseller-tag) to uniquely identify their specific customer AS to the IXP, so that the MAC address of the Ethernet frame corresponds to the reseller's router. Fig. 1 illustrates this second approach, where reseller J allows customer ASes F and G to reach other members. When the reseller transmits these packets into the IXP, the reseller also pushes a tag (reseller-tag) to uniquely identify their specific customer AS to the IXP. The IXP bridges traffic into the IXP switching fabric by removing the outer-most reseller-tag while keeping the IXP-tag. In Fig. 1, the sFlow tap sees the IXP-tag and the MAC address of the reseller, which uniquely identifies the AS that sent the packet.

A reseller can also provide remote peering to members colocated at one IXP that want to reach members in a different IXP. Fig. 1 shows a more complicated example, where AS E bridges their network between metropolitan regions using the services of a reseller (K) present at both IXPs.

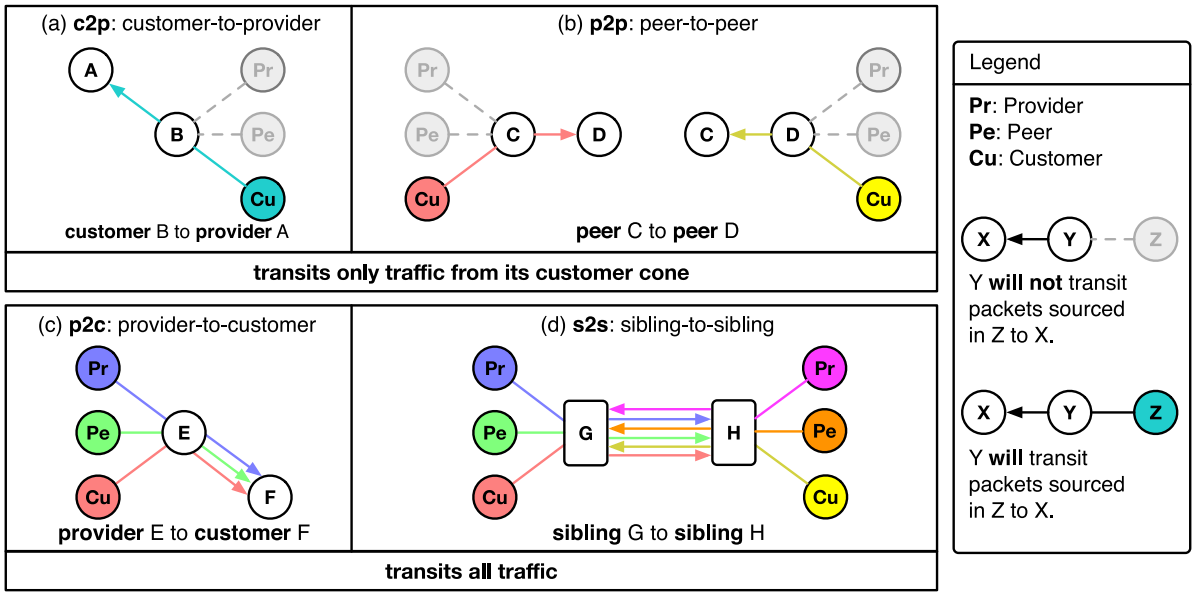


Fig. 2. The customer cone constrains the set of source addresses expected in valid inter-domain traffic transiting an AS behaving rationally in a c2p or p2p relationship. In the c2p relationship shown in (a), B transits traffic from its customers to A, but not its peers and providers. Similarly, in the p2p relationship shown in (b), C only transits traffic from its customers to D (likewise, from D to C). However, as shown in (c), the p2c relationship does not constrain the source addresses transited by E to F, and neither does the s2s relationship between G and H in (d).

2.4. AS relationships and customer cones

The three primary classes of AS relationships are customer-provider (c2p, p2c), peering (p2p) and sibling (s2s). In a c2p relationship (also known as transit), a customer buys access to achieve global reachability to all routed Internet address space. In a p2p relationship, two ASes agree to exchange traffic destined to prefixes they or their customers own, typically without either AS paying the other [48]. In a s2s relationship, a single organization operates both ASes, and may transit packets received from any source.

An AS's *customer cone* includes all ASes reachable through its customer ASes, i.e., direct and indirect customer ASes (in other words, ASes reachable only through p2c links) [17]. The customer cone constrains which source IP addresses one should see in valid inter-domain traffic transiting from a customer to its provider, or between peers. Fig. 2 illustrates the subtleties: an AS in a c2p or p2p relationship with another AS should only send packets with a source address from within its customer cone — respectively, (a) and (b) in Fig. 2. In contrast, a link between a provider to its customer or between two siblings may forward packets with *any* routed source address — (c) and (d) in Fig. 2.

2.5. Measuring deployment of SAV

Many academic research efforts have described techniques to promote deployment of SAV [49–52]. Fewer efforts have tried to empirically measure SAV compliance for networks attached to the global Internet. In 2005, Beverly, et al. developed a client–server technique to allow users to test networks to which they are currently attached [53], and operationalized a platform to track trends over time [10,11]. The platform allows for inference of deployed SAV policy, but has limited coverage, because it relies on users downloading and running measurement software. To overcome this limitation, researchers have recently investigated techniques to infer lack of SAV using macroscopic Internet data sets. In 2017, Lone et al. reported a technique to infer spoofed traffic in massive traceroute archives, based on the assumption that an edge network should never appear to be providing transit in a traceroute path [54]. This method is limited by whatever appears in the traceroute archives, and can be hampered by traceroute artifacts caused by inconsistent Internet Control Message Protocol (ICMP) implementations in routers [55].

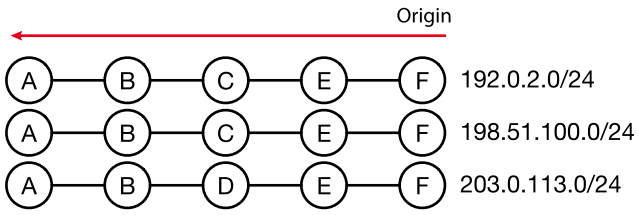
Most closely related to our study, in 2017 Lichtblau et al. used a large IXP as a vantage point for inferring which networks at the IXP had not deployed SAV [16]. For each member at the IXP, their method infers a set of IP prefixes containing addresses that may legitimately appear in the source field of IP packets crossing an IXP. They infer that a member AS that sends a packet into the IXP switching fabric with a source address outside of those prefixes has not deployed SAV. They argued against using AS relationships and AS customer cones which they claimed did not address asymmetric routing. However, their method did not consider ASes forming customer–provider or sibling relationships at the IXP, where all routed addresses may be legitimate source addresses in IP packets crossing an IXP — (c) and (d) in Fig. 2. In these cases, there is no way to infer SAV deployment across these links at the IXP.

3. Tackling methodological challenges

We describe the core of our methodology in the context of two complex groups of challenges to inferring spoofed traffic in IXP traffic data. The first one (Section 3.1) is determining which addresses are valid source addresses in traffic transiting a given neighbor AS, i.e., packets with a source address that is *in-cone* for that AS. An incomplete set of valid addresses could yield false inferences of failure to deploy SAV, should a valid address appear in the observed packets but not be in the in-cone set, i.e., be *out-of-cone* for that AS. The second group of challenges (Section 3.2) is navigating the analytical implications of modern IXP interconnection practices that can impede the visibility of both topology and traffic. These practices complicate the analysis of which ASes exchanged traffic and their routing relationship. Once we address these challenges, the remainder of our method is IXP-specific but straightforward, and we describe it in Section 4.

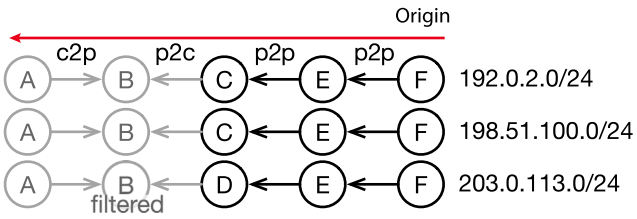
3.1. Subtleties in cone construction

Inferring the set of valid source addresses for packets traveling from a specific AS to a specific adjacent AS at an IXP requires navigating a multidimensional parameter space. Precision in this process is crucial. Mistakenly excluding valid addresses could result in a misclassification of an AS as not performing source address validation (false positive).



ASes	Full Cones:
A, B, E, F	192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24
C	192.0.2.0/24, 198.51.100.0/24
D	203.0.113.0/24

Fig. 3. Example full cones (Section 3.1.1) for six ASes given these BGP paths. The full cone for an AS includes every prefix that contains that AS in the path for all routes observed by public route collectors, regardless of the underlying relationships.



ASes	AS-Level Customer Cones:
A, B, F	(contain only themselves with these paths)
C	C, E, F
D	D, E, F
E	E, F

ASes	Prefix-Level Customer Cones:
A, B	(empty with these paths)
C, D, E, F	192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24

Fig. 4. Example customer cones (Section 3.1.2) for six ASes using the same BGP paths from Fig. 3. In customer cone construction, we annotate each AS link with a c2p, p2c, or p2p relationship before inferring the prefix-level customer cone. With this specific set of paths, AS B is filtered out of the process (the PPCC cone construction uses routes observed from its providers and peers), and AS A has no customers or peers considering only these BGP paths.

Similarly, including invalid source addresses could result in spoofed packets going undetected (false negatives). As mentioned in Section 1, there is no global registry that contains ground truth on which addresses are valid source addresses for packets transited by an AS; instead, we must infer them from BGP routing data sources [56–58], even though these sources may contain spurious announcements [59].

3.1.1. Full cone

The full cone (used in [16]) is the more permissive of the two construction methods. Aiming to minimize false positives, Lichtblau et al. chose to *"not distinguish between peering/sibling, customer–provider and provider–customer links. Rather, whenever [the algorithm sees] two neighboring ASes on an AS path, [the algorithm] presumes a directed link between the two, where the left AS is considered upstream of the right AS"*. The resulting cone for an AS, which they call its *full cone (FC)*, includes every prefix that contains that AS in the BGP route's AS path [16], for all routes observed by public route collectors in Routing Information Base (RIB) snapshots and updates during the measurement period.

They acknowledged that this method intentionally sacrifices specificity, i.e., inflating the address space considered legitimate for each AS pair, in the interest of avoiding false positives, i.e., avoiding mistakenly attributing a failure to deploy SAV. Using this method, a stub AS that provides a public BGP view containing all prefixes it received from its peers and providers will have *all* of these prefixes included in its full cone, i.e, the entire routed address space will be deemed valid. Fig. 3 illustrates the full cones for six ASes; if A were a stub AS and a customer of B, all three prefixes would be included in A's full cone even though no system in A should originate packets with those source addresses.

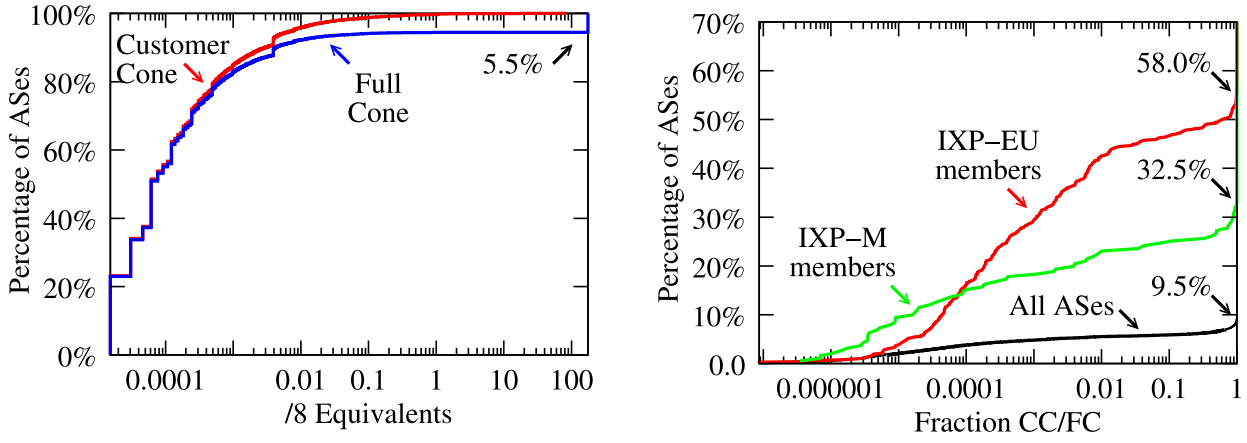
3.1.2. Customer cone

The customer cone is the more restrictive of the two construction methods; it takes into account the semantics of AS relationships. As described in Section 2, the AS-level customer cone defines the set of ASes reachable using customer links from the AS, including the AS itself [17]. We use the *provider/peer-observed customer cone* (PPCC) algorithm defined in [17] to build an AS-level customer cone. Using the paths in Fig. 4, the PPCC method constructs the cone of AS C using routes observed from its providers and peers. The PPCC method accommodates hybrid relationships, where an AS may not propagate all of its customer routes to all of its peers and providers. Customer cone inference critically relies on accurate routing relationship inferences; a customer link incorrectly inferred to be a peer link will result in address space that the provider AS transits being incorrectly excluded from its customer cone. Fig. 4 illustrates the AS-level customer cones for the same ASes and paths as Fig. 3, with link annotations to identify the inferred routing relationships between ASes. However, an AS-level customer cone does not define the set of valid source addresses in traffic transiting a given neighbor AS.

Once we have the AS-level customer cone for C, we transform it into its corresponding prefix-level cone by including all prefixes originated by ASes in the AS-level customer cone for C during the same observation window. This novel prefix-level cone construction accommodates traffic engineering practices, where an AS may announce different prefixes through different providers, but forward traffic from within these prefixes according to the best route to the destination. To illustrate, in Fig. 4, we include 203.0.113.0/24 in C's prefix-level customer cone, even though that prefix is not observed in any BGP paths involving C, because F is in C's customer cone. Importantly, we do not include these three prefixes in A's customer cone, because A has no customers. We also combine the prefix-level customer cones of siblings, because a sibling C may transit packets from the customer cone of any of C's siblings to C's peers or providers.

3.1.3. Impact of the cone construction method

Fig. 5 shows how the choice of cone construction method impacts inference of valid address space for all ASes (Fig. 5(a)) and for the ASes at the IXP-EU used in [16] and the IXP-M in our study (Fig. 5(b)), in both cases using traffic and BGP data from April 2017 (see Section 5 for further detail on the datasets we used). In particular, 5.5% of all ASes in the Internet had a full cone that contained all routed address space. For 90.5% of ASes, the full cone and customer cone were congruent (included the same addresses), but 58% of IXP-EU member ASes had full cones covering more addresses than the customer cone, and 42% of ASes had an FC 100 times larger than their CC. This disparity of cone sizes for all ASes compared to those at the IXP is because while over 80% of the Internet's ASes are stubs, i.e., do not provide transit, these are less likely to peer at an IXP. Further, IXPs are popular places to operate public route collectors because the collector can obtain BGP routing views from multiple ASes at a single place. Therefore, those ASes at an IXP that provide a routing view will have all of the prefixes they announce in routes to the collector, including those from their peers and providers, in their full cone. Fig. 6 shows how the choice of BGP observation window impacts [60] the inference of out-of-cone traffic at IXP-M in Brazil in April 2017 using the full cone. This effect is



(a) Absolute Cone Sizes.

(b) Relative Cone Sizes.

Fig. 5. The cone construction approach (Section 3.1) significantly impacts the source addresses each method will consider valid. In (a) we show that 5.5% of all ASes had the equivalent of all routed addresses (175/8 equivalents) in their full cone in April 2017. In (b) we show that while 90.5% of ASes had (full and customer) cones covering the same set of addresses, 58% of the IXP-EU members would have covered more addresses, with 42% of ASes having a full cone 100 times larger than their customer cone. Note, per discussion in Section 3.2, an AS announcing 0.01%/8 equivalents is announcing less than 0.006% of the routed address space.

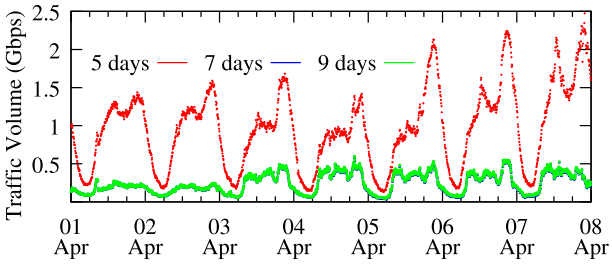


Fig. 6. The inferred out-of-cone traffic volume for the full cone is sensitive to changing BGP observation window sizes in the construction of the cone. While the 7 and 9 day lines are almost identical, the 5-day line contains an order of magnitude more traffic because the set of valid addresses for each AS is smaller. In Section 7 we discuss the differences in traffic magnitude between the two cone construction methods — Full Cone and Customer Cone.

because of the FC's permissive nature, which exposes the cone inference to announcements across the whole Internet.

Neither the full cone nor the customer cone handle the complexities that sibling ASes (ASes under the same ownership) bring. Because siblings may provide mutual transit to each other, the set of valid addresses that can transit between each AS is the entire routed address space. To observe this behavior in public BGP data, which both the FC and CC use, would require a view from each sibling AS. Current sibling relationship inference methods [61,62] use WHOIS data, which is not only inconsistently formatted across regions, but also becomes stale if not updated as mergers occur, leading to false and missing inferences [62].

3.2. Topology and traffic visibility

While the original role of IXPs was to promote peering between ASes physically present and connected to a switching fabric, in practice IXP services have become more complicated. For example, many networks now obtain transit services from a provider at the IXP [14]. Or, an organization can connect its sibling networks using the IXP switching fabric. IXPs may also offer services such as remote peering and layer-2 transport, as well as virtualized segmenting of traffic into multiple VLANs. These services present three challenges to accurate inference of SAV deployment.

First, the BGP routing relationship between two IXP members impacts whether the customer cone can constrain inference of valid source address space. As discussed in Section 2.4, a provider AS may forward packets with a source address from any routed prefix in the Internet to their customer, and a sibling may forward packets from the provider of one sibling to the customer of another sibling. In these cases, we cannot apply a cone of valid addresses to infer the SAV policy of the transmitting member. We can only make this inference when that member has a peering or transit relationship with another member. In contrast to prior work [16], we consider the routing relationship between the two IXP member ASes exchanging traffic when evaluating the source address of a packet crossing the IXP.

Second, there are traffic visibility impediments. As discussed in Section 2.3, traffic between members connected to the same switch will stay within the switch. In a distributed switching fabric (more details in Section 10), observing all member traffic requires traffic capture from all switches. Similarly, ASes may establish private interconnections with other ASes at the same colocation facility; their traffic exchange does not use the core IXP switching fabric. Further, to infer SAV policy of an IXP member, we require hosts in the cone of the IXP member to attempt to send spoofed packets to hosts they would reach across the IXP. Because most ASes peer at an IXP, only destinations in the customer cone of the receiving AS would receive that packet, i.e., the victim or the amplifier must be reached via the IXP. Because most customer cones are small (Fig. 5(a), where only 5% of ASes have more than 0.006% of the routed address space in their customer cone) the chance of a victim or amplifier also being reached via a peering relationship at the IXP is small; a victim or amplifier is more likely to be reached via a transit relationship at the IXP.

Third, shared use of IXP ports creates attribution challenges. While the IXP can supply the AS number of record for a given port, with the associated Ethernet MAC address, that port does not necessarily uniquely identify the sending AS when a reseller uses the port to provide layer-2 transport, in cases of remote peering and port resale (Section 2.3), or when the port connects to another exchange. Prior work has illustrated measurement challenges of inferring remote peering [42,43]. In this work, both IXPs (IXP-M and IXP-L) provided us the reseller and IXP tags they used to bridge remote peers. This IXP-specific knowledge exemplifies why we believe a customer-cone-based approach to SAV inference will ultimately be integrated into expert system capabilities rather than be amenable to complete layer-3 automation.

4. Implementing classification pipeline

The customer cone construction method described in Section 3 underpins our traffic classification method — how we infer invalid

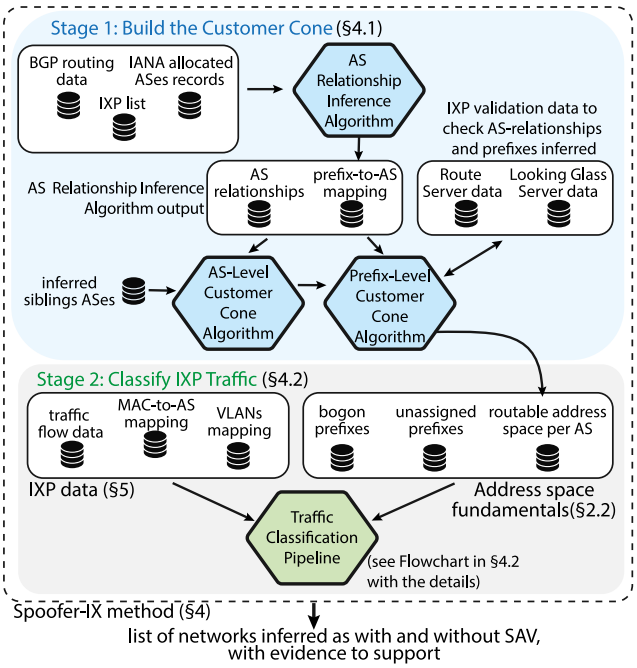


Fig. 7. Spoofer-IX inference method overview.

source addresses (presumably spoofed) in packets crossing an IXP, and the ASes responsible for transmitting them. We describe how these pieces fit together in our system implementation, which relies on IXP traffic measurements and topological information, i.e., BGP data and IXP switching fabric forwarding databases. The implementation, illustrated in Fig. 7, has two stages: (1) build an accurate *prefix-level customer cone* from BGP data, and (2) verify that the customer cone can serve to constrain our inference, and if so classify traffic as *in* or *out* of the transmitting AS's customer cone.

4.1. Stage 1: Build the customer cone

The first stage has three phases, as follows.

Phase 1: Filter and Sanitize AS Paths. To avoid incorrectly identifying non-existent links between ASes, we use the method from [17] to discard paths with artifacts, such as loops, non-adjacent Tier-1 ASes, and reserved/unassigned ASes [63]. We also discard paths to prefixes longer than /24 or shorter than /8.

Phase 2: Infer AS Relationships. We use the sanitized AS Paths from phase 1 to derive AS relationships on a weekly basis, also according to the algorithm in [17]. This algorithm applies heuristics to annotate each AS link with either a transit (C2P, P2C) or peering (P2P) relationship.

Phase 3: Construct the Prefix-Level Customer Cone. An AS's *prefix-level customer cone* is the set of prefixes covering source addresses from the AS and its customers, for which the AS will transit traffic. Conceptually, constructing this cone is the most complicated part of our method, and where mistakes can hinder accuracy. We construct a prefix-level customer cone using the method described in Section 3.1.2.

4.2. Stage 2: Classify IXP traffic

The second stage has three phases, illustrated in Fig. 8.

Phase 1: Filter Bogon and Unassigned Addresses. We first classify traffic with *bogon* and *unassigned* source IP addresses, according to Team Cymru [64], as described in Section 5. Networks sending packets with unassigned source IP addresses are unlikely to have implemented SAV correctly, since the most obvious implementation blocks traffic from such addresses because they are not routed, therefore have no feasible return path. This phase is independent of any routing semantics, unlike the subsequent two phases, which consider the sending and receiving ASes for the monitored link, the routing relationship between them, and the prefix-level customer cone of the sending AS.

Phase 2: Filter Unverifiable Packets. This phase classifies traffic flows as suitable to inference of spoofing using the customer cone, marking unsuitable traffic as *Unverifiable*. Verifiable traffic must satisfy all of the following:

1. It must have a valid MAC-to-AS mapping for both the sending and receiving MAC addresses.
2. It must not have a known router IP address in the source IP address of the packet. Such a source IP address could be from any interface on the router, which might be assigned by an AS whose address space is not in the customer cone of the router's owner.
3. It must not have a known IP address of the IXP LAN prefix. These prefixes are assigned to the IXP operator and should not be publicly announced, but sometimes member ASes mistakenly announce them.
4. It must not have a source MAC address from a remote peer or layer-2 transport provider.
5. It must not have a source MAC address from a known provider or sibling of the receiving AS.

Phase 3: Classify Packets with Customer Cone. The remaining traffic has a MAC-to-AS mapping, and is either transmitted by a customer of a transit provider at the IXP, or by a peer of another AS at the IXP. If a relationship was not visible in BGP, then we assume the traffic between these members was p2p and use the cones to classify the traffic exchanged. For these transmitting ASes, we classify traffic as *in-cone* or *out-of-cone* using the prefix-level customer cone (henceforth *customer cone* or *CC*) created in the previous stage. We classify a packet whose source IP belongs to the sending AS's customer cone address space as *in-cone*. Otherwise, we classify the packet as *out-of-cone*.

4.3. Using spoofer-IX implementation

We developed Spoofer-IX as a set of tools to enable other researchers and network infrastructure operators to use our inference method. Fig. 9 depicts the implementation of Spoofer-IX in five steps. A full-run of Spoofer-IX is comprised of all five steps. Note that the same set of steps can be employed to distinct network infrastructures (see details in Section 10). However, as discussed in Section 3, precise knowledge about the network topology and interconnections is required to obtain robust inferences from Spoofer-IX. In the following, we present implementation details of each step.

Step 1. Prepare datasets (Section 5). To obtain accurate results, it is important to align the time windows of the datasets. We provide helper scripts to download, prepare, and optimize datasets, and also to automate topology information extraction from various of switch manufacturers using Python's Netmiko [65] and Google's TextFSM [66] libraries. We also make available helper scripts (using the Python Scrapy library [67]) that download and process the BGP routing data files from public BGP route collectors [56,57] to build the cones.

Step 2. Execute cone construction in three phases (Stage 1, Section 4.1). The codebase of this stage is written in Perl. This step starts with the filtering and sanitization of AS Paths from the previously downloaded BGP data files. Then, proceeds with the execution of the AS Relationships inference algorithm. Lastly, the construction of the Prefix-Level Customer Cone.

Step 3. Execute traffic classification pipeline (Stage 2, Section 4.2 and Fig. 8). The core implementation of the pipeline and the next steps

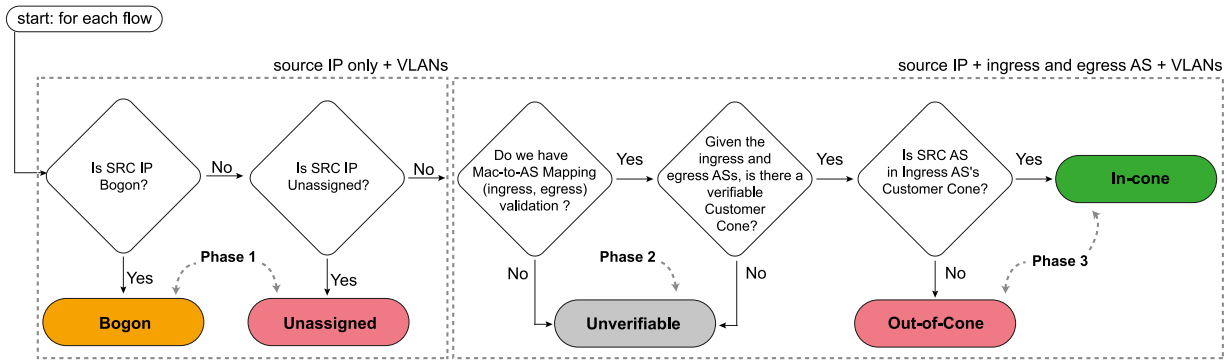


Fig. 8. Flowchart showing our traffic classification pipeline (stage 2 of methodology, described in Section 4.2).

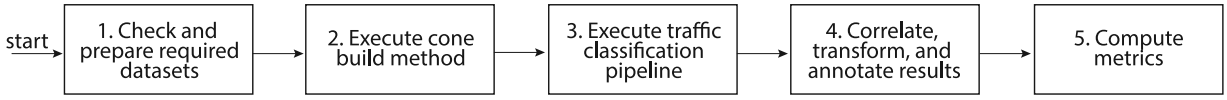


Fig. 9. Overview of the global steps composing the Spoofer-IX methodology.

(4 and 5) were developed in Python, and some additional Bash helper scripts are used to automate parameterized execution. This step saves classification results to disk in Apache Avro [68] format for use in the next step.

Step 4. Correlate, transform, and annotate results. Using the classification results and correlation datasets (e.g., MAC-to-AS mapping, prefix-to-AS mapping), create intermediate files with additional information to compute metrics. Forward results to a transformation process that classifies traffic and computes metrics for different granularities across space (e.g., IP address, prefix, AS) and time (e.g., 5-min, 15-min, 1-hour).

Step 5. Compute metrics. Use data created in previous step to look for atypical network events that suggest attacks. Use two metrics to assess IPv4 address usage over time: Activity and Churn, and Spatio-Temporal Properties [69,70]. The former reflects the volatility of address activity over time, while the latter captures aggregated properties of active IPs seen in each time granularity.

We provide an automatic and personalized mode for use in a multiprocessing desktop environment. For the automatic setup, we provide a Bash helper script to install and configure dependencies (e.g., NFDUMP [71], Apache Avro [68], RIPE NCC BGPdump [72]), enabling its use out-of-the-box, e.g., on a fresh Linux Ubuntu server. The source code and the documentation are available online at [21].

5. Datasets

IXP-BR: traffic and routing data. We collected datasets from two Brazilian IXPs [30], with different purposes. First, IXP-M transports up to 200 Gbps among 200+ members, allowing an in-depth evaluation of the proposed method. IXP-L, on its turn, has over 1600 members and transports up to 6 Tbps, allowing an evaluation at scale, focused on feasibility. We record traffic data using sFlow [35] with a sample rate of 1:4096 packets. From the medium-sized IXP, we use two uninterrupted sFlow datasets, from April 1 to June 5 2017 (10 weeks), and May 1 to June 5 2019 (5 weeks). From the large IXP, we examine traffic exchanged during one day (April 12, 2018) in three distinct Colocation Facilities that constitute part of its switching fabric infrastructure.

Topology data over connectivity fabric. The source and destination IP addresses in the IP headers of the observed packets contain the communication endpoints, which are unlikely to be the pair of member ASes sending and receiving those packets across the IXP fabric. To infer these ASes, we used layer-2 information (i.e., MAC addresses) in the packets. To map MAC addresses to sending and receiving ASes of each flow (the MAC-to-AS mapping), we relied on information from the forwarding database of each switch that is part of the IXP switching fabric.

Router IP addresses. For comparability with previous work [16], we used CAIDA's Internet Topology Data Kit (ITDK) [73] to identify router interface IP addresses. We used the ITDK snapshot closest in time to the IXP traffic capture window. We considered traffic from ITDK-inferred router interfaces to be *unverifiable* (Section 4.2) because the source IP address could be from any of the interfaces of the router, and thus might be assigned by an AS whose address space is not in the Customer Cone of the router's owner (Section 4.2).

Bogons and unassigned addresses. We used Team Cymru's Fullbogons feed [64,74] to filter out traffic with source IP addresses that are bogons (e.g., private, special use, reserved) [25,26,75] or unassigned. Unassigned prefixes are allocated by IANA to an RIR [27,28], but not subsequently assigned by the RIR to an end-user (e.g., an ISP) [13]. We used the lists compiled by Team Cymru in each 4h interval per day for the same time windows as our IXP traffic data collection.

Public BGP Data. Our traffic filters rely on Customer Cones inferred from public BGP routing table snapshots collected by Route Views (RV) and RIPE's Routing Information Service (RIS) [56,57]. We downloaded one BGP RIB table per day from all available (18 and 16 in 2017/2018, 19 and 18 in 2019 from RIS and RV, respectively) collectors for the same time windows as our traffic data. We extracted all AS paths in these tables that announced reachability to IPv4 prefixes, repeating this process for each week.

AS Siblings. We used CAIDA's AS to Organization classification of ASes into sets that likely belong to the same organizations [62]. CAIDA's method parses the Regional Internet Registries' WHOIS dumps and delegation files to create a unified mapping between ASes and organization names, then uses hints in the name strings, delegation files, identifiers, and email addresses to infer AS sets with common ownership. For each measurement period, we used the AS-to-Organization mapping that CAIDA constructed using WHOIS data collected closest to the traffic capture window.

6. Inferring spoofed traffic at IXPs

We applied our method to classify traffic from IXP-M. We present results obtained from longitudinal traffic classification and discuss

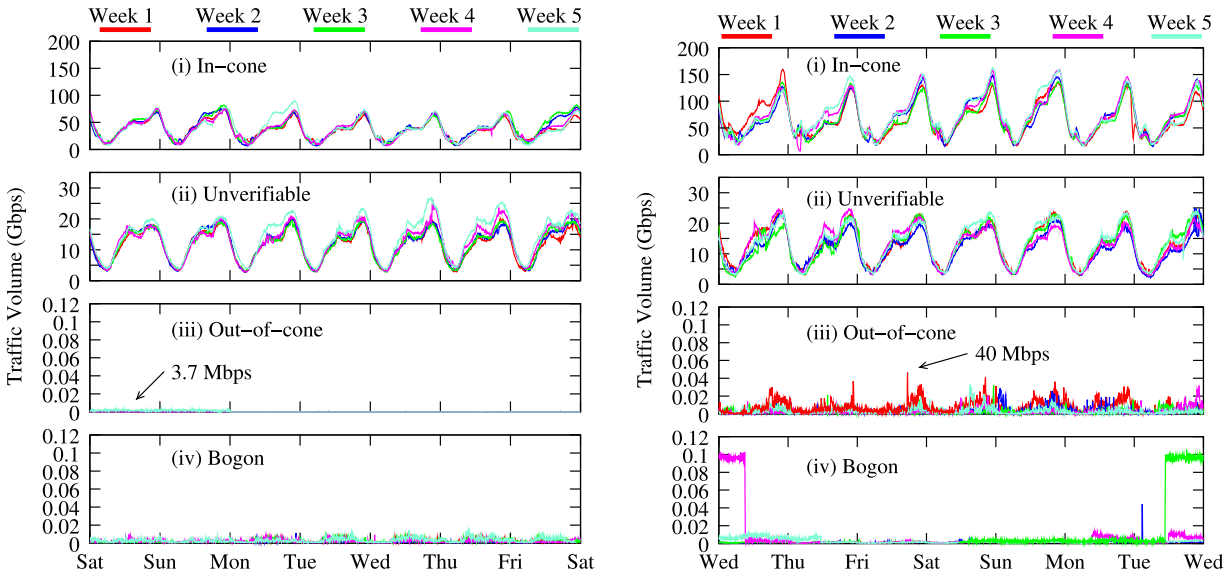


Fig. 10. Five weeks of traffic for 2017 and 2019 classified with our method. We omit the unassigned class, which is negligible. For all ten weeks, we inferred almost no out-of-cone traffic — a maximum of 40 Mbps for an IXP with a peak of 200 Gbps.

Table 1
Unique AS pairs observed exchanging traffic at IXP-M in each 5-week period. Approximately 1.4% of AS pairs had a non-p2p relationship. (This IXP was rearchitected in early 2019, which may explain the drop in observed peers.)

Relationship	April 2017		May 2019	
p2p	19,161	(98.7%)	12,057	(98.4%)
p2c	222	(1.1%)	183	(1.5%)
s2s	21	(0.1%)	10	(0.1%)
total	19,404		12,250	

properties of the traffic we classified as unverifiable traffic. We cross-check our inferences against active measurements of spoofing from CAIDA's Spoofer project [11].

6.1. Longitudinal traffic classification

Fig. 10 shows the volumes of traffic we classified for two five-week periods in 2017 and 2019, showing that our results are consistent across these time periods. In 2017, the peak rate across the core switch during our observation period was 120 Gbps. In 2019 the peak had grown to 200 Gbps, and as expected most traffic (84.65%) across the exchange was classified as in-cone.

In 2017, the peak out-of-cone traffic we inferred was 3.7 Mbps, and in 2019, 40 Mbps. We believe these values are upper-bounds for out-of-cone traffic at the IXP-M core switch, and we derived these volumes after investigating the underlying properties of traffic between pairs of members, in rank order of contribution to the out-of-cone traffic volume at the IXP. For packets with characteristics not typically associated with spoofing, e.g., a Transmission Control Protocol (TCP) packet with payload, or packets toward a known transport provider, we manually investigated the relationships between the ASes exchanging the packet. We found 27 sibling ASes in 11 distinct organizations that exchanged traffic across IXP-M but were missing from CAIDA's public AS-to-Org dataset (Section 5). To determine which ASes were siblings, we consulted the official website of those ASes to find information on their ownership, contacted the ASes directly to inquire, or contacted the IXP operators to understand the relationship between two ASes at the IXP. Further, through the IXP-M operators, we approached 36 members, and 34 of them responded with explanations of the behavior we saw.

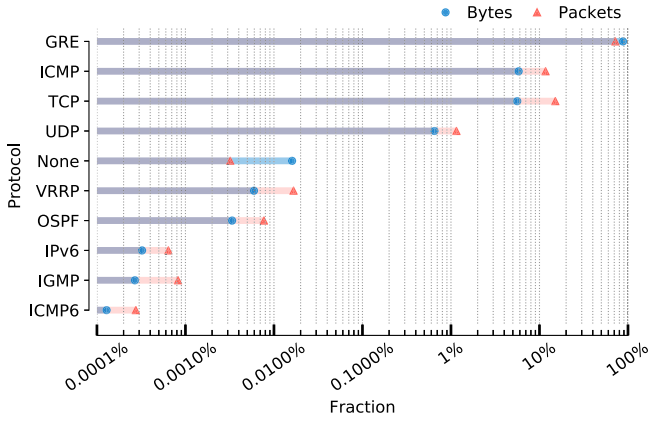


Fig. 11. Transport protocols mix seen in the Bogon traffic at IXP-M (Week-1, May 2019), bytes and packets. List of protocols ordered by bytes.

Although the number of members was similar between 2017 and 2019 (208 and 203, respectively), 28 new members were present in the 2019 analysis. We found that the increase in out-of-cone traffic between 2017 and 2019 was due to additional complex relationships and traffic transport agreements between members in the 2019 data that were not visible to the IP layer or in the BGP protocol (more details in Section 8). Table 1 summarizes the number of unique AS pairs we observed to exchange traffic for the five-week periods beginning 1 April 2017 and 1 May 2019. While we inferred more than 98% of the AS pairs had a p2p relationship, approximately 1.4% of AS pairs had a different class of relationship that impacted our ability to infer SAV policy of the transmitting AS.

Fig. 10 also shows the volume of traffic with bogon source addresses, with a peak of approximately 100 Mbps across the exchange for the Wednesday at the end of week 3 (10(b)-iv). We found 38.9% to be ICMP, TCP, and User Datagram Protocol (UDP). We found these networks deliberately used as source addresses the private range (RFC1918) to tunnel traffic between members. The use of Generic Routing Encapsulation (GRE) and IP-in-IP represented 61.1% of the traffic. We observed the same behavior in distinct weeks. Fig. 11 shows the list of transport protocols we observed in Bogon traffic in the first

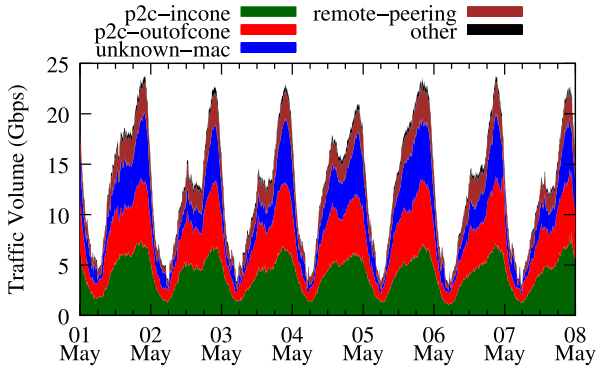


Fig. 12. Classification of unverifiable traffic at IXP-M. 61.8% of the unverifiable traffic was sent by a provider to a customer across the exchange. Because a provider can transit packets from any source address in the Internet, there are no invalid addresses that would allow detection of spoofed packets. For completeness, we further classified traffic from each provider as being in or out of their customer cone.

week of May 2019. GRE dominated this category, with more than 87% of bytes and 72% of packets, representing 1.56 TB of absolute traffic in that week. The other significant fraction used ICMP and TCP protocols, accounting for some 11.43% of the exchanged bytes. Other protocols such as UDP, VRRP, and OSPF accounted for roughly 0.68% of bytes exchanged at the IXP. The *None* category includes malformed packets, i.e., those with no valid data in the packet header. These may happen due to network equipment error during packet handling (e.g., processing overload, firmware bug).

6.2. Unverifiable traffic breakdown

For both the 2017 and 2019 observation periods, there was a peak of approximately 25 Gbps of unverifiable traffic across the exchange, representing 15.3% of total traffic crossing IXP-M at that time (Figs. 10(a)-ii and 10(b)-ii).

Fig. 12 classifies traffic for the first week of May 2019. 61.9% of the unverifiable traffic was sent from a provider to a customer across the exchange, where no cone of valid addresses applied (Section 2.4). If we had applied the customer cone approach to this p2c traffic, we would have inferred 52% of it was from within the provider's customer cone, with the remaining 48% of traffic from outside the provider's customer cone. Because a provider can transit packets to its customers from any source address in the Internet (Section 2.4), there are no invalid addresses that would allow inference of spoofed packets. This potential for erroneous inference is why we must classify all packets from a transit provider to a customer as unverifiable. Another 21.4% of the unverifiable traffic was because we did not have an AS mapping for either the source or destination MAC addresses (IXP-M lacked historical data for this mapping), and for 14.1% of traffic we could not determine the origin AS because the source MAC address and VLAN tag indicated the traffic was from a remote peering provider. Finally, all of the other categories summed to only 2.6% of the traffic, so we do not discuss these categories further.

6.3. Cross-checking against active measurements

We inferred out-of-cone traffic for 38 of the 203 members (18.7%) at IXP-M between 1 May and 5 July 2019 (most recent 5 weeks of traffic). Of the 203 members, 35 (17.2%) were also in CAIDA's public Spoofer dataset [11], which requires a volunteer to have been present in the network. The active measurement test run explicitly sends packets with spoofed source addresses to CAIDA's servers, to test SAV deployment of the that network (Section 2.5). Table 2 summarizes the (in) congruity between the two datasets. Of the 35 ASes that

Table 2
Congruity between CAIDA's public spoofer dataset and inferences using IXP-M traffic. Of the 35 ASes observed in both data set, CAIDA's spoofer dataset inferred 54% of them had not deployed SAV, because CAIDA received a packet with a spoofed source address. Only 4 of these 35 (11%) were observed to forward an out-of-cone packet into the IXP; 2 of these 4 were in CAIDA's spoofer dataset as not deploying SAV.

Spoofer-CAIDA	Spoofer-IX		Sum
	In-cone	Out-of-cone	
Spoof-received	17	2	19 (54.3%)
Spoof-blocked	14	2	16 (45.7%)
Sum	31 (88.6%)	4 (11.4%)	35

overlapped, CAIDA's Spoofer dataset indicated 54% of them had *not* deployed SAV. Only 4 of these 35 ASes (11%) were inferred by Spoofer-IX to forward an out-of-cone packet into the IXP, implying that IXPs alone may not provide effective visibility into SAV deployment, because participants were not forwarding spoofed packets, at least during our five-week observation window.

The difference does not mean that either methodology is flawed. Instead, each method has its own requirements and coverage: the presence of spoofed traffic is a condition for Spoofer-IX, as much as CAIDA's Spoofer requires each participant to install client software and send packets. In fact, these results show that these methodologies complement each other. CAIDA's Spoofer covers only 17. 2% of the members of the IXP-M, while Spoofer-IX enable the analysis of all members and their traffic in its entirety.

7. Spoofer-IX vs. full cone inference

Fig. 13 shows the volume of out-of-cone traffic inferred by both the Spoofer-IX and full cone methods for traffic data captured during the first week of May 2019. The Spoofer-IX method inferred a peak of 40 Mbps of out-of-cone traffic (best seen in Fig. 10(b)), whereas the full cone method inferred a peak of 2.5 Gbps, an order of magnitude disparity between these two methods. The diurnal pattern of the inferred out-of-cone traffic (Fig. 13(b)(i)) is consistent with user-based traffic patterns, with no observable peaks suggesting a volumetric spoofed-source attack launched from within member ASes of the IXP. The second row of Fig. 13 shows churn in source IP addresses [69,76] seen in each five minute window. For the full cone method, the absolute volume of source addresses observed follows the traffic volume profile as a whole, and is concentrated in 20–40 ASes per five minute window, which is not a typical pattern of attacks that utilize randomly-spoofed source addresses.

Analysis of discrepancy in classification results. The discrepancy in traffic volumes classified as out-of-cone by these two methods derives from the full cone method classifying some provider-to-customer traffic as being out-of-cone (Section 2.5), whereas the Spoofer-IX method, which takes customer semantics into account, classified provider-to-customer traffic as unverifiable. Fig. 12 shows Spoofer-IX classified 1–5 Gbps of out-of-cone traffic from providers to customers as unverifiable. When we classified the full cone's out-of-cone traffic using the Spoofer-IX method, 92.6% of the traffic was from a provider to a customer across the exchange, carrying 0.5–2 Gbps of traffic (Fig. 14).

Finally, the traffic volume classified as in-cone by the full cone method is larger than that by the Spoofer-IX method. 85.5% of the traffic that the full cone method classified as in-cone was also classified as in-cone by the Spoofer-IX method, with the remaining 14.5% classified as unverifiable by Spoofer-IX. Fig. 15 shows how the Spoofer-IX method classified 59.9% of this unverifiable traffic as from a provider to a customer across IXP-M, and 26.4% of the unverifiable traffic as out-of-cone for the provider. We hypothesize that this traffic is classified as in-cone for the full-cone method because some provider ASes (or their customers) provided a BGP view, so the full cone included these addresses as in-cone for these provider ASes (Section 3.1.3). Note that

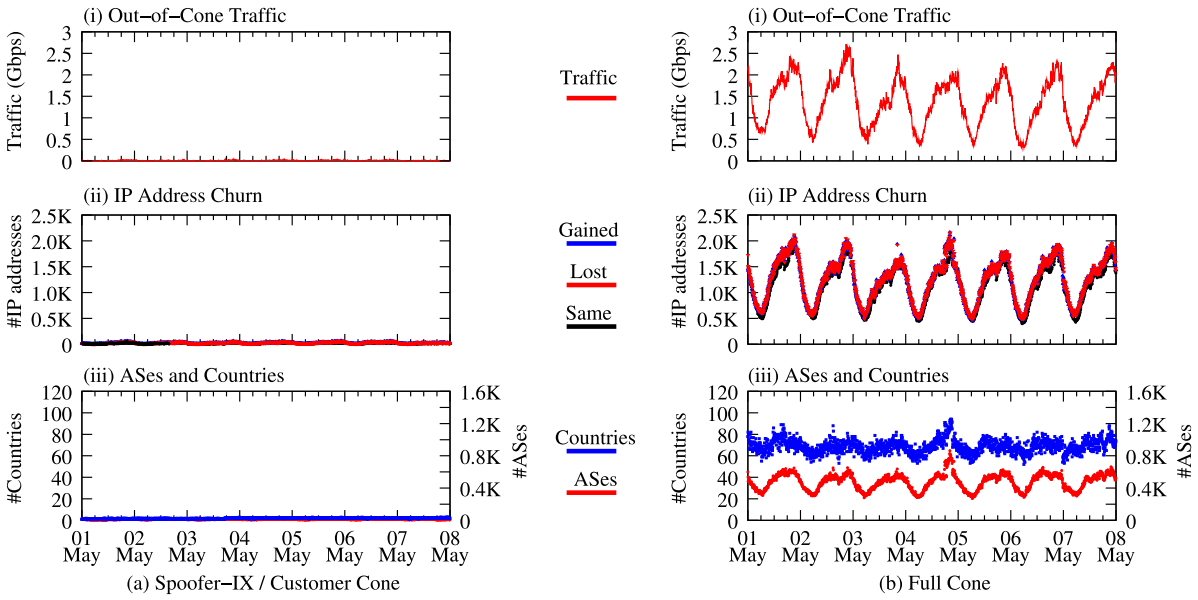


Fig. 13. Comparison of metrics for out-of-cone traffic inferred by the Spoofer-IX and full cone methods for the first week of May 2019. We compute each metric per 5-minute window of traffic data, and use the same range on Y axes between methods to allow for comparison. For IXP-M, the full cone method inferred an average of 1.5 Gbps of out-of-cone traffic, whereas our method inferred a maximum of 40 Mbps (best seen in Fig. 10(b)-iii).

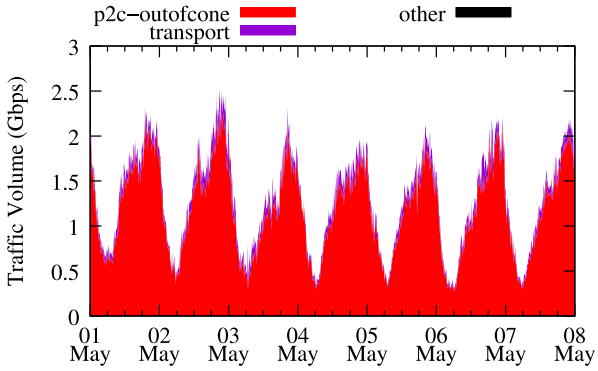


Fig. 14. Spoofer-IX classification of traffic classified as out-of-cone by the full cone method. Spoofer-IX infers that 92.6% of this out-of-cone traffic was from a provider to customer across IXP-M, and therefore unverifiable, because a provider can transit traffic from any source IP address to their customer, and it is therefore not feasible to identify spoofed packets by their source IP address alone.

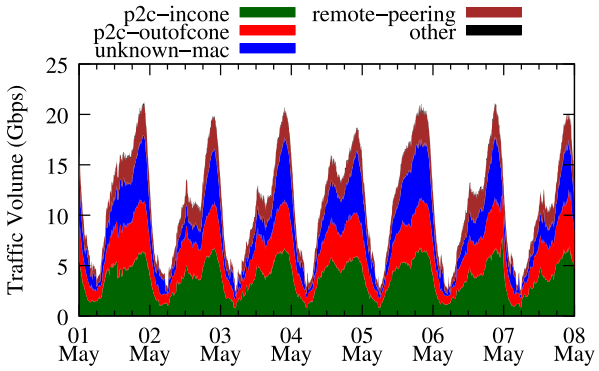


Fig. 15. Classification of in-cone traffic for the full cone that Spoofer-IX classified as unverifiable. The traffic profile is similar to that in Fig. 12, with some unverifiable provider-to-customer traffic classified as out-of-cone by the full cone method (Fig. 14).

the traffic profiles in Figs. 12 and 15 are similar: the discrepancy is mostly due to the full cone method classifying some of Spoofer-IX's unverifiable provider-to-customer traffic as out-of-cone (Fig. 14). However, all routed addresses may be legitimate source addresses in IP packets crossing an IXP from a provider to customer, and no cone of valid addresses can infer the SAV policy of the provider for these packets.

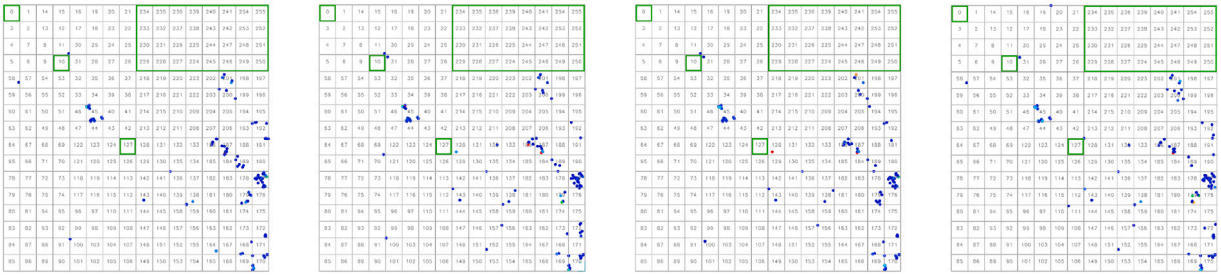
8. Looking at the out-of-cone traffic nature

As discussed in Section 6 we believe we inferred an upper bound on out-of-cone traffic crossing the IXP-M core switch, but the actual value is likely lower. To confirm our intuition, we manually searched for patterns consistent with attack traffic behavior, e.g., flooding amplification. To represent the results, we used Hilbert Curves [77,78] to visualize IPv4 address usage in this out-of-cone category.

Fig. 16 shows four Hilbert heatmaps, one per day, from Week-1 of May 2019. The IPv4 address space is rendered in two dimensions using a space-filling continuous fractal Hilbert curve [77,78] of order 16. Each square in the figure represents a /8 IP prefix block, numbered by its first IPv4 octet. Each colored dot represents how many IP source addresses appeared in traffic within a given /16 from each block, with blue and red reflecting low (from 1) and high counts (above 255), respectively. The color white means no packets with a source address in the /16 block. The green rectangular shapes denote IETF-reserved address blocks [27].

We observe a clear diurnal pattern of IP address space usage across hours and days, suggesting that this out-of-cone traffic is legitimate and not associated with attacks. The plots show no random exploration of the IP space (e.g. multicast IP ranges, reserved blocks, and military prefixes) which might indicate an attack [79].

We examined the top five prefixes by usage of their IP space. We checked their AS owners, as well as those ASes' business type classification. For packets with source addresses within these top prefixes, we examined the corresponding ingress AS crossing the IXP-M infrastructure. In the list of ingress ASes, we found regional ISPs present at more than one IXP and engaged in complex relationships hard to classify automatically. By carefully investigating these relationships, we found ASes associations (i.e., multiple ASes sharing dynamically infrastructure and links) leveraging transport providers to reach their



(a) May 01 (b) May 03 (c) May 05 (d) May 07

Fig. 16. Hilbert heatmap visualization showing the utilization of the address space in out-of-cone traffic (Week-1, May 2019). The IPv4 address space is rendered in two dimensions using a space-filling continuous fractal Hilbert curve [77,78] of order 16. Each square in the figure represents a /8 IP prefix block, numbered by its first IPv4 octet. Each colored dot represents how many source IP addresses appeared in traffic within a given /16 from each block. The level of activity is indicated by colors, from blue (low) to red (high), with green, yellow and orange as moderate levels, and white meaning no packets with a source address in the /16 block. Green boxes denote IETF-reserved address blocks.

intended destinations — limiting our methodology automatic inference capacity, requiring a manual investigation like this one to understand the traffic behavior properties.

9. Filtering consistency by IXP members

In the previous sections, we examined the traffic properties, made inferences about lack of SAV and the incidence (or lack of) attacks exploiting spoofing during the observation considered. We take a higher-level perspective to answer two questions. First, how consistent are filtering policies across AS members of the IXP? Second, can we observe SAV adoption increasing over time? In both cases, we hope for opportunities for IXPs coordinators to help members improve SAV compliance, or for IXP members to collectively improve IXP policies in the interest of global Internet security.

9.1. Filtering consistency across ASes

Fig. 17 presents a Venn diagram of percentage of members at the IXP contributing traffic to the distinct categories, as well as intersections in contributions. The results in the plot refer to all packets observed during the 5-week period in 2019. For each packet, we used its category (as defined in Section 4, see Fig. 8) and MAC-to-ASN mapping (Section 5) to identify the member AS emitting these packets. As in previous work [16], the percentages reflect lower bounds on which filtering strategy member ASes apply, as an AS may not send flows with spoofed source IP addresses across the IXP during our observation window. We argue that these lower bounds are usefully tight given the length of the observation period (15 weeks, spanning two years at IXP-M).

Interestingly, not all members appear as sources of traffic. Out of 204 active members during the five weeks in 2019, 154 (75.5%) members appeared as a source of traffic at IXP-M. From those 154 ASes, we found that 15% did not send any traffic classified as either out-of-cone, bogon, or unassigned, i.e., their traffic was clean. On the other end of the spectrum, we find 0.7% of members contributing traffic to all four categories. In other words, at least one network did not perform any filtering. Around 1.3% of participants contributed only bogon traffic. Via IXP-M we notified these networks about the anomaly; according to operators of the networks involved, the problem was caused by an updating procedure in routers accidentally deleting the filter for bogon ranges. A single AS member contributed packets in the unassigned category. This same member also sent out-of-cone, bogon, and in-cone packets. No member contributed only out-of-cone traffic exclusively. Almost 23% (35 members) contributed with in-cone, out-of-cone and bogon packets, while 58.8% (90 members) contributed both in-cone and bogon traffic. Lastly, 1.3% (2 members) contribute to in-cone and out-of-cone traffic.

Considering all 200+ members at IXP-M, few contributed with potentially spoofed traffic. Recall that filtering bogon traffic requires

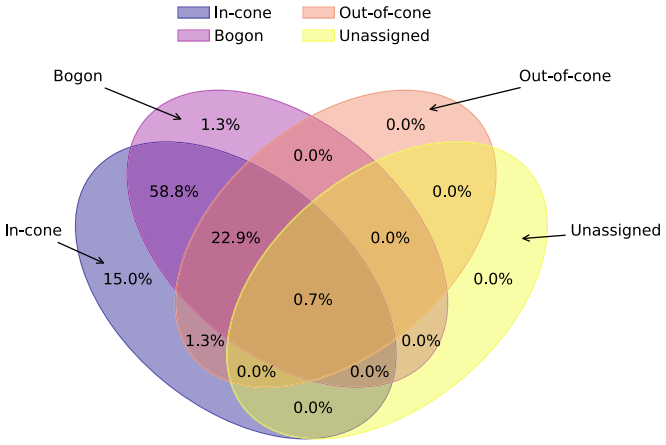


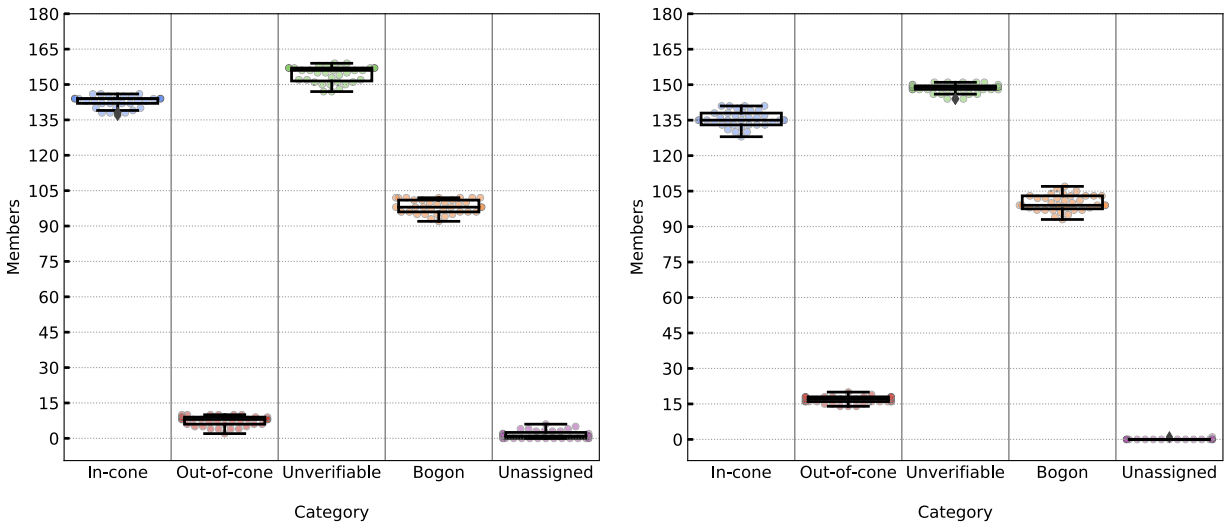
Fig. 17. Venn Diagram of members contributing traffic to four categories: in-cone, out-of-cone, bogon and unassigned. Analyzes performed for five-week period of 01 May 2019 to 05 June 2019.

relatively static filters that do not need frequent updating as topology and customers change (Section 2.1). In contrast, SAV filtering (of out-of-cone traffic) requires updating filters as business dynamics change. It thus surprised us to see more networks exchanging bogon traffic than out-of-cone traffic. We explained this mystery with our previous discovery that AS members occasionally use bogon source IPs to exchange traffic via tunneling protocols (e.g., GRE, IP-in-IP) with another member at the same switching fabric. Nevertheless, the presence of out-of-cone traffic suggests that those member ASes sending it do not strictly enforce SAV according to the BCPs [3,4].

9.2. Stability of SAV over time

We investigated stability of SAV filtering configuration over time at IXP-M. Fig. 18 shows a Swarm plot (i.e., a categorical scatterplot) overlapped with a Box plot considering the values of all categories (in-cone, out-of-cone, unverifiable, bogon, unassigned). Each circle in the swarm indicates the total number of members per day over five weeks of 2017 (Fig. 18(a)) and another five weeks of 2019 (Fig. 18(b)). Box plot values show the minimum, maximum, average (square), median (line inside square), lower (25th) and higher (75th) quartiles for the number of IXP members over time in each category.

Even with two years between the traffic observation periods, the overall behavior was stable for all categories. This result is consistent with the fact that networks do not give a high priority to remediation [9]. Typically operators minimize interventions to deployed operational devices to avoid service disruptions. These results are



(a) May 1 - Jun 5, 2017. (b) May 1 - Jun 5, 2019.

Fig. 18. Swarm Box plot reflecting configured filtering practices over time. It shows the scatterplot distribution per category of the total number of members per day over five weeks of 2017 18(a) and five weeks of 2019 18(b). The points represent the results of each day adjusted (along the categorical axis) to avoid overlap. The box plot presents the minimum, maximum, median (line inside square), lower (25th) and higher (75th) quartiles for the number of IXP members over time in each category.

consistent with those observed by active measurements [11]. The maximum and minimum values of each category have little to no difference. The highest standard deviation among categories is 3.38 (bogon category, Fig. 18(b)), where we observed deliberate use of these prefixes with tunneling protocols (Section 6).

This data indicates that the level of deployment of SAV in the observed networks did not increase when comparing the periods in 2017 and 2019. We cannot conclude that this behavior applies to the Internet as a whole, or will persist, but based on the present evidence we cannot be optimistic about networks voluntarily increasing protection against IP spoofing attacks.

10. Scaling spoofer-IX to more complex IXP architectures

We explored practical application and generalizability of our Spoofer-IX method and implementation to larger and more complex IXP infrastructures. In this context we believe the critical question lies in the feasibility of splitting the flow data collection across switching peering fabrics. Our goal is to maximize the ability for any networks on the Internet to detect and filter spoofed traffic, including IXPs with diverse interconnection practices and network topologies that hinder the deployment of IP-based measurement methodologies.

To this end, we extended the Spoofer-IX implementation to be more flexible about input parameters, and to run using information (i.e., traffic flow data, topology information, and MAC-to-ASN mapping from members) from individual networks. To explore a case study, we partnered with a second, larger IXP in Brazil. At the time of our analysis, IXP-L had over 30 colocation facilities and 150 switches, with more than 1600 member ASes. We collaborated with three colocation facilities that constitute part of this second IXP. We collected traffic flow data from eight switches spread across these distinct facilities, as well as topology and MAC-to-ASN mapping information. We executed our method individually across each switch. This capability to perform traffic analysis per switch enables us to scale execution of our method to much larger peering fabrics, lowering the barrier to deploy the method, and enabling SAV compliance enforcement at individual colocation facilities associated with an IXP. The steps are the same as for IXP-M, where we collected traffic at the single core switch.

The process of bootstrapping the execution of our methodology (step 1, Section 4.3, Fig. 9) is mostly shared between all runs, if the traffic flow period matches for all switches. The exceptions are local information regarding the network and the switch under analysis. Cone construction (step 2) occurs once, and all executions share the results, which must correspond to the timeframe of the traffic and BGP data. Subsequent steps (3 to 5) are straightforward executions of our classification pipeline, followed by data transformations and metrics computation across the prepared data.

To perform the traffic classification step we used the same server employed for analysis of IXP-M, as follows. There were two processors Intel Xeon E5-2640 v4 2.4 GHz–40 threads, with 64GB RDIMM RAM memory, and 1TB SSD SATA storage and 3 disks of 1.2TB of 10 K RPM. It took on average 40 min to classify one day of traffic flow data. The existing traffic classification algorithm implementation has linear time ($O(n)$), where n represents the length of each sFlow dataset. Each 5-min file per colocation facility on IXP-L contained on average 106,552 flows, with constant time operations performed using efficient in-memory data structures. The algorithm takes constant extra space, because the amount of additional memory needed does not vary with the number of flows processed. Instead, it varies according to the amount of memory required to load the base filtering datasets (Bogon prefixes list, Unassigned prefixes feed, ITDK Routers IPs, Sibling ASes list, IXPs ASes and their LAN prefixes) as well as the correlation datasets (IANA/RIRs available blocks, IP Geolocation databases, Prefix-to-AS hashmap). The current prototype implementation has not been optimized; obvious gains are possible in terms of time and space complexity, e.g., through extra filtering on datasets pre-loads and advanced network flow record data structures.

Table 3 summarizes the classification results we observed during one day in April 2018 for each switch in the partnered facilities. It shows the set of switches grouped by colocation facility, the max and average traffic rate in Gbps, the average percentage of traffic found in each category, and the time (in seconds) to execute the classification. We analyzed traffic sent by 485 members in total. As expected, we classified the majority of traffic as valid (in-cone). Moreover, no traffic was classified as spoofed. Through discussions with the IXP-L coordinators, we hypothesize that the stricter set of policies adopted by this IXP lead to a more secure infrastructure. Among their policies, they have a "quarantine network" for new members. It is an isolated network that every new member must first connect in order to perform a validation of the security properties and configurations, before they are allowed to join the shared switching fabric with all other members. IXP-L also implements a policy to drop traffic matching bogon prefixes [80]. Based

Table 3
One day of traffic for individual switches of three distinct colocation facilities of a large IXP in Brazil, classified with our Spoofer-IX method. We omit the bogon, unassigned and out-of-cone classes since nothing was detected.

Facility	Switches	Max traffic rate	Average traffic rate	Average % in-cone traffic	Average % unverifiable traffic	Time to execute
CF1	SW1	684 Gbps	398 Gbps	94.16%	5.84%	4066.28 s
	SW2	99 Gbps	32 Gbps	68.18%	31.82%	2923.12 s
CF2	SW1	7 Gbps	5 Gbps	88.36%	11.64%	865.28 s
	SW2	10 Gbps	7 Gbps	90.2%	9.8%	537.65 s
	SW3	43 Gbps	28 Gbps	73.88%	26.12%	777.54 s
	SW4	33 Gbps	20 Gbps	88.14%	11.86%	1123.05 s
CF3	SW1	341 Gbps	192 Gbps	86.53%	13.46%	3008.04 s
	SW2	557 Gbps	309 Gbps	96.18%	3.81%	2967.50 s

on Table 3, we notice that switches CF1-SW2 and CF2-SW3 had a higher average of unverifiable traffic, which was due to high levels of provider-to-customer traffic compared to other switches. In contrast, CF1-SW1, CF3-SW1 and CF3-SW2 handled the highest volumes, being responsible for delivering the traffic of big content providers to IXP members.

Applying the Spoofer-IX method and system to the IXPs was a frustrating experience, requiring that we overcome many challenges, including: (1) policy enforcement, e.g. NDA agreements to obtain access to traffic and topology data; (2) evolving processes and architecture within the IXPs, e.g. obtaining up to date topology information; (3) interfacing with running systems and distinct device manufacturers; and (4) handling system failures and data problems. Besides, as discussed before (Section 3.2), configuring the collection of traffic flow data is not trivial. It is fundamental to understand the IXP infrastructure topology organization, and the cooperation of the many colocation facilities involved to correctly configure all switches avoiding or being aware of duplicated flow records, i.e., flows that traverse multiple sampling points. These challenges will characterize any modern interconnection environment, and navigating them is an integral aspect of successfully executing this sort of analysis. We see great potential in enabling execution of our methodology across as broad a set of networks as possible, including IXPs distributed across many colocation facilities and switch fabrics. The modular decomposition of our approach, including bootstrapping and data preparation steps, promotes this generalizability and broad impact. This case study demonstrated that the Spoofer-IX methodology and system implementation can handle the analysis of much larger network infrastructures, even beyond IXPs.

11. Discussion

Challenges of Validation. We could not acquire ground truth data to validate our results, in part due to the negligible amount of out-of-cone traffic we observed, and the challenge of asking any network to validate a small volume of packets. We instead verified that our prefix-level customer cone inferences (Section 3.1.2) were consistent with BGP data extracted from the IXP's route servers. The only inconsistencies we found were due to ASes that had been returned to their RIR and still appeared in public BGP announcements, but did not appear in routes from the IXP route servers.

Generality of the methodology. Assessing the generality of our approach requires applying our method to traffic from more IXPs, which is challenging because it requires the cooperation of other IXP operators. In pursuit of generalizability, we designed and developed Spoofer-IX to accommodate the Best Current Operational Practices (BCOPs) defined by a group of IXPs [18,29] that describe how IXP operators should securely configure IXPs, including VLANs and route servers. We believe our methodology can be applied to a variety of IXPs, and demonstrated an example (Section 10). More generally, any other method to infer spoofed traffic in IXP traffic data must address the same challenges we encountered. All heuristics defined during the analysis of IXP-M were applicable to IXP-L, exactly the way they were defined. The same applies to our study of the distinct snapshots (2017, 2019) of the traffic from IXP-M. The discussion in Section 3.2 reflects on the challenges IXP infrastructures pose and which we dealt through our methodology. Following, we point out the manual effort required regarding datasets.

Applying our method requires two data sets: the traffic data sets, and the metadata that maps IXP infrastructure — VLAN tags on each packet, and MAC addresses to ASes. Our method is automated except for inference of the siblings (Section 6), which requires some manual effort. However, there are a wide variety of IXP architectures that affect traffic visibility (Section 3.2), and new IXP architecture innovations to support advanced services will require careful consideration of their impact on our method. Our use of traffic characterization was limited to the packet headers available to us; full payload would enable improvements in traffic analysis, and additional cross-checks.

Emerging IXP trends and their impact on the inference of SAV policy. New IXP services allow networks to self-provision private, on-demand bandwidth in seconds between data center locations (a.k.a., colocation facilities) or cloud service providers, [44,81–84]. In 2019, AMS-IX, DE-CIX and LINX joined to develop an API to provision and configure interconnection services at multiple IXPs [85]. The resulting IX-API [86] will allow users to manage their interconnection services, from ordering new ports, to configuring, changing, and canceling services at multiple IXPs. These proposals share a common goal: enable a more dynamic resilient interconnection environment, where networks and IXPs can adapt to changing conditions. They do not propose to change methods to implement the configurations tackled in this paper, but rather create abstractions to facilitate configuration changes.

12. Concluding remarks

The use of IXPs as a focal point for SAV deployment has received recent attention by both the research [16] and policy communities [87–89]. However, inferring SAV deployment at an IXP is remarkably challenging, more so than has been captured in the literature, due to a combination of operational complexities that characterize today's interconnection ecosystem, and the inherently heuristic nature of topology and traffic inferences on persistently opaque network infrastructure. Many of our discoveries were eye-opening, although not cause for optimism for those interested in infrastructure protection.

First, although we approached this project aware of several methodological challenges for inferring spoofed packets at IXPs, the reality was more daunting. We recognized the importance of using the semantics of AS relationships, which is conceptually straightforward but even more painstakingly complicated in practice than we expected. We designed, implemented, and applied a method that accounts for both epistemological and operational challenges, and showed how this method reveals inaccuracies in previous methods that are agnostic to AS relationship semantics.

But we also found epistemological challenges remain. While we inferred out-of-cone traffic with our method at our two IXPs, there are still edge cases we have not yet explained, as some of the traffic appears to have signatures of legitimate traffic. More importantly, further effort is required to understand the degree to which any IXP could be used as

a SAV deployment lens. We publicly release our code [21] in hopes that other researchers and IXPs will use it to further improve our collective ability to measure and expand deployment of SAV filtering. Finally, this work illustrates the deep subtleties of scientific assessments of operational Internet infrastructure, which exemplifies the persistent tension between the need for reproducibility of methods and results [22,23,90], and the opacity of commercial infrastructure.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback on our research. We are also thankful to Leandro Bertholdo, Bruno Lorensi, Cesar Loureiro, Julio Sirota, Milton Kashiwakura, Demi Getschko – all from IX.br – for their support, feedback, and discussions that allowed this work to be possible. This material is based in part on research sponsored by the Department of Homeland Security (DHS), United States of America Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, United States of America, Cyber-Security Division via contracts, United States of America D15PC00188 and 140D7018C0010, the National Science Foundation (NSF), United States of America via awards OAC-1724853 and OIA-1937165, Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Brazil grant 310408/2017-2, and by CAPES/Brazil via Finance Code 001. The published material represents the position of the authors and not necessarily that of the sponsors.

References

[1] R. Morris, A weakness in the 4.2BSD unix TCP/IP software technical report 117, AT&T bell laboratories, 1985.
[2] S.M. Bellovin, Security problems in the TCP/IP protocol suite, ACM SIGCOMM Comput. Commun. Rev. 19 (2) (1989) 32–48.
[3] P. Ferguson, D. Senie, Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing, 2000, RFC 2827 (BCP 38). Updated by RFC 3704.
[4] F. Baker, P. Savola, Ingress filtering for multihomed networks, 2004, RFC 3704 (BCP 84).
[5] T. Scheid, Defending the olympics from DDoS, 2016, https://blog.apnic.net/2016/10/17/defending-olympics-ddos/.
[6] S. Kottler, February 28th DDoS incident report, 2019, https://githubengineering.com/ddos-incident-report/.
[7] C. Morales, NETSCOUT Arbor confirms 1.7 Tbps DDoS attack; The terabit attack era is upon us, 2019, https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/.
[8] O. Klaba, 1.3Tbps DDoS mitigated by our VAC, 2019, https://twitter.com/olesovhcom/status/969328679410110466.
[9] M. Luckie, R. Beverly, R. Koga, K. Keys, J.A. Kroll, k claffy, Network hygiene, incentives, and regulation: Deployment of source address validation in the internet, in: ACM SIGSAC Conference on Computer and Communications Security (CCS), 2019.
[10] R. Beverly, A. Berger, Y. Hyun, k. claffy, Understanding the efficacy of deployed internet source address validation filtering, in: ACM Internet Measurement Conference (IMC), 2009, pp. 356–369.
[11] CAIDA, CAIDA Spoofer project, 2019, https://www.caida.org/projects/spoofer/.
[12] APNIC, Weekly routing table report, 2019, http://thyme.apnic.net/current/data-summary.
[13] The Number Resource Organization, NRO extended allocation and assignment reports, 2019, https://www.nro.net/statistics/.
[14] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, W. Willinger, Anatomy of a large European IXP, in: ACM SIGCOMM, 2012, pp. 163–174.
[15] L. Müller, M. Luckie, B. Huffaker, K. Claffy, M. Barcellos, Challenges in inferring spoofed traffic at IXPs, in: Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies, in: CoNEXT '19, ISBN: 9781450369985, 2019, pp. 96–109, http://dx.doi.org/10.1145/3359989.3365422, https://doi.org/10.1145/3359989.3365422.
[16] F. Lichtblau, F. Streibelt, T. Krüger, P. Richter, A. Feldmann, Detection, classification, and analysis of inter-domain traffic with spoofed source IP Addresses, in: ACM Internet Measurement Conference (IMC), 2017, pp. 86–99.
[17] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, k. claffy, AS relationships, customer cones, and validation, in: ACM Internet Measurement Conference (IMC), 2013, pp. 243–256.
[18] Internet Society, MANRS IXP programme, 2019, https://www.manrs.org/ixps/.
[19] D. Freedman, B. Foust, B. Greene, B. Maddison, A. Robachevsky, J. Snijders, S. Steffann, Mutually agreed norms for routing security (MANRS) implementation guide, 2019, https://www.ripe.net/publications/docs/ripe-706.
[20] Job Snijders, Practical everyday BGP filtering: Peer locking (NANOG67), 2016, https://www.youtube.com/watch?v=CSLpWBrHy10.
[21] L. Müller, M. Luckie, B. Huffaker, kc claffy, M. Barcellos, Spoofer-IX sourcecode, 2019, https://github.com/spoofer-ix/spoofer-ix.
[22] V. Bajpai, A. Brunstrom, A. Feldmann, W. Kellerer, A. Pras, H. Schulzrinne, G. Smaragdakis, M. Wählisch, K. Wehrle, The dagstuhl beginners guide to reproducibility for experimental networking research, ACM SIGCOMM Comput. Commun. Rev 49 (1) (2019) 24–30.
[23] V. Bajpai, O. Bonaventure, k. claffy, D. Karrenberg, Encouraging reproducibility in scientific research of the internet, Dagstuhl Rep. 8 (10) (2019) 41–62.
[24] Internet Society, Mutually agreed norms for routing security (MANRS), 2019, http://www.manrs.org/manrs.
[25] R. Moskowitz, D. Karrenberg, Y. Rekhter, E. Lear, G. de Groot, Address allocation for private internets, 1996, RFC 1918 (BCP 5).
[26] M. Cotton, L. Vegoda, E. R. Bonica, B. Haberman, Special-purpose IP address registries, 2013, RFC 6890 (BCP 153). Updated by RFC 8190.
[27] IANA, IANA IPv4 address space registry, 2019, https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml.
[28] IANA, Internet protocol version 6 address space, 2019, https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml.
[29] Euro-IX, IXP BCOPS (best current operational practices), technical recommendations, 2019, https://www.euro-ix.net/en/forixps/set-ixp/ixp-bcops/technical-recommendations/.
[30] IX.br, IX.br – internet exchange Brazil, 2019, http://ix.br.
[31] DE-CIX, DE-CIX Internet exchange, 2019, https://www.de-cix.net/en/.
[32] AMS-IX, Amsterdam internet exchange (AMS-IX), 2019, https://www.ams-ix.net/.
[33] LINX, London Internet exchange (LINX), 2019, https://www.linx.net/.
[34] IX.br Forum 12, Remote peering panel with DEC-ix, AMS-ix, LINX and ix.br, 2019, https://www.youtube.com/watch?v=K283b3AKZ94.
[35] P. Phaal, S. Panchen, N. McKee, Inmon corporation's sflow: A method for monitoring traffic in switched and routed networks, 2001, RFC 3176.
[36] B. Claise, Cisco systems netflow services export version 9, 2004, RFC 3954.
[37] N. Chatzis, G. Smaragdakis, A. Feldmann, W. Willinger, There is more to IXPs than meets the eye, ACM SIGCOMM Comput. Commun. Rev. 43 (5) (2013) 19–28.
[38] Euro-IX, IXP BCOPS (best current operational practices), 2019, https://www.euro-ix.net/en/forixps/set-ixp/ixp-bcops/.
[39] DE-CIX, DEC-IX Metrovlan, 2019, https://www.de-cix.net/en/de-cix-service-world/metrovlan.
[40] AMS-IX, AMS-IX Private interconnect service, 2019, https://www.ams-ix.net/ams/service/private-interconnect.
[41] LINX, LINX Private VLAN, 2019, https://www.linx.net/products-services/private-vlan/.
[42] I. Castro, J.C. Cardona, S. Gorinsky, P. Francois, Remote peering: More peering without internet flattening, in: ACM Conference on Emerging Networking EXperiments and Technologies (CoNEXT), 2014, pp. 185–198.
[43] G. Nomikos, V. Kotronis, P. Sermpezis, P. Gigis, L. Manassakis, C. Dietzel, S. Konstantaras, X. Dimitropoulos, V. Giotsas, O Peer, Where Art Thou?: Uncovering remote peering interconnections at IXPs, in: ACM Internet Measurement Conference (IMC), 2018, pp. 265–278.
[44] Megaport, Megaport - A better way to connect, 2019, https://www.megaport.com.
[45] IX Reach, IX Reach remove peering services, 2019, https://www.ixreach.com/services/remote-peering/.
[46] LINX, Connexions at London internet exchange point, 2019, https://www.linx.net/join-linx/connexions/.
[47] AMS-IX, AMS-IX Partner program, 2019, https://www.ams-ix.net/ams/partners.
[48] L. Gao, On inferring autonomous system relationships in the internet, IEEE/ACM Trans. Netw. 9 (6) (2001).
[49] Z. Duan, X. Yuan, J. Chandrashekar, Constructing inter-domain packet filters to control IP spoofing based on BGP updates, in: IEEE INFOCOM, 2006, pp. 1–12.
[50] A. Yaar, A. Perrig, D. Song, StackPi: New packet marking and filtering mechanisms for ddos and IP spoofing defense, IEEE J. Sel Areas Commun. (2006) 1853–1863.
[51] X. Liu, A. Li, X. Yang, D. Wetherall, Passport: Secure and adoptable source authentication, in: USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2008, pp. 365–378.
[52] B. Liu, J. Bi, A.V. Vasilakos, Toward incentivizing anti-spoofing deployment, IEEE ToIFS (2014) 436–450.
[53] R. Beverly, S. Bauer, The spoofer project: Inferring the extent of source address filtering on the internet, in: USENIX Steps to Reducing Unwanted Traffic on the Internet (SRUTI), 2005.

[54] Q. Lone, M. Luckie, M. Korczyński, M. van Eeten, Using loops observed in traceroute to infer the ability to spoof, in: Passive and Active Measurement (PAM), 2017, pp. 229–241.

[55] A. Marder, M. Luckie, A. Dhamdhere, B. Huffaker, J. Smith, k claffy, Pushing the boundaries with bdrmapIT: Mapping router ownership at internet scale, in: ACM Internet Measurement Conference (IMC), 2018.

[56] RIPE, Routing information service (RIS), 2019, http://www.ripe.net/ris/.

[57] University of Oregon, Route views project, 2019, http://www.routeviews.org/.

[58] PCH, Raw routing data, 2019, https://www.pch.net/resources/Raw_Routing_Data/.

[59] M. Luckie, Spurious routes in public BGP data, ACM SIGCOMM Comput. Commun. Rev. 44 (3) (2014) 14–21.

[60] G. Comarela, G. Gürsun, M. Crovella, Studying interdomain routing over long timescales, in: ACM Internet Measurement Conference (IMC), 2013, pp. 227–234.

[61] X. Cai, J. Heidemann, B. Krishnamurthy, W. Willinger, Towards an AS-to-organization map, in: ACM Internet Measurement Conference (IMC), 2010, pp. 199–205.

[62] B. Huffaker, K. Keys, R. Koga, M. Luckie, kc claffy, CAIDA inferred AS to organization mapping dataset, 2019, https://www.caida.org/data/as-organizations/.

[63] IANA, Autonomous system (AS) numbers, 2019, https://www.iana.org/assignments/as-numbers/as-numbers.xml.

[64] Team CYMRU, The bogon reference, 2019, http://www.team-cymru.com/bogon-reference.html.

[65] K. Byers, Netmiko, 2019, Available at http://ktbyers.github.io/netmiko/.

[66] Google, Textfsm, 2019, Available at https://github.com/google/textfsm.

[67] Scrapinghub, Scrapy, 2019, Available at https://scrapy.org.

[68] Apache, Apache avro, 2019, Available at https://avro.apache.org.

[69] P. Richter, G. Smaragdakis, D. Plonka, A. Berger, Beyond counting: New perspectives on the active IPv4 address space, in: ACM Internet Measurement Conference (IMC), 2016, pp. 135–149.

[70] A. Dainotti, K. Benson, A. King, k. claffy, M. Kallitsis, E. Glatz, X. Dimitropoulos, Estimating internet address space usage through passive measurements, ACM SIGCOMM Comput. Commun. Rev 44 (1) (2013) 42–49.

[71] P. Haag, nfdump, 2019, Available at https://github.com/phaag/nfdump.

[72] RIPENCC, BGPdump, 2019, Available at https://bitbucket.org/ripencc/bgpdump-hg/wiki/Home.

[73] CAIDA, The CAIDA internet topology data kit, 2019, http://www.caida.org/data/internet-topology-data-kit.

[74] Team CYMRU, Ipv4 fullbogons, 2019, https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt.

[75] J. Weil, V. Kuarsingh, C. Donley, C. Liljenstolpe, M. Azinger, IANA-Reserved ipv4 prefix for shared address space, 2013, RFC 6598 (BCP 153).

[76] K. Benson, A. Dainotti, k. claffy, A.C. Snoeren, M. Kallitsis, Leveraging internet background radiation for opportunistic network analysis, in: ACM Internet Measurement Conference (IMC), 2015, pp. 423–436.

[77] J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, J. Bannister, ANT Censuses of the internet address space, 2019, Available at https://ant.isi.edu/address/index.html.

[78] D. Wessels, kc claffy, Mapping the IPv4 address space, 2019, Available at https://www.caida.org/research/id-consumption/census-map/.

[79] M. Majkowski, The real cause of large ddos - IP spoofing, 2018, https://blog.cloudflare.com/the-root-cause-of-large-ddos-ip-spoofing/.

[80] IX.br, Programa por uma Internet mais Segura – Ações no IX.br, 2019, http://old.ix.br/doc/acoes-seguranca-ix-br-20180927.pdf.

[81] P. Marcos, M. Chiesa, L. Müller, P. Kathiravelu, C. Dietzel, M. Canini, M. Barcellos, Dynam-IX: A dynamic interconnection eXchange, in: ACM Conference on Emerging Networking EXperiments and Technologies (CoNEXT), 2018.

[82] Epsilon, Epsilon telecommunications limited – connectivity made simple, 2019, www.epsilontel.com/.

[83] PacketFabric, Packetfabric, 2019, https://www.packetfabric.com/.

[84] Console, Console - the cloud connection company, 2019, https://www.consoleconnect.com/.

[85] Lynsey Buckingham, IX-API For the good of the internet, 2019, https://www.linx.net/ix-api-for-the-good-of-the-internet/.

[86] AMS-IX and DE-CIX and LINX, IX-API Simplify your IX services, 2019, https://ix-api.net/.

[87] Internet Society, IXP Participants, 2019, https://www.manrs.org/participants/ixp/.

[88] Tech Accord, Cybersecurity tech accord, 2019, https://cybertechaccord.org/.

[89] NIC br, Programa por uma internet mais segura, 2019, https://bcp.nic.br/i+seg/.

[90] J. Eumann, R. Hiesgen, T.C. Schmidt, M. Wählisch, A Reproducibility Study of "IP Spoofing Detection in Inter-Domain Traffic", in: ACM Internet Measurement Conference (IMC), Posters Reproducibility Track, 2019, https://arxiv.org/abs/1911.05164.

Lucas Müller holds a Ph.D. in Computer Science from the Federal University of Rio Grande do Sul (UFRGS), Institute of Informatics, Brazil. During his doctoral studies, he also worked at the Center for Applied Internet Data Analysis (CAIDA) at the University of California San Diego (UCSD) studying the inter-domain IP Spoofing problem under the supervision of Kc Claffy, Matthew Luckie, Bradley Huffaker, and Marinho Barcellos. His research interests are in large-scale network measurements and analysis of Internet interconnections, particularly from a security perspective. He received his B.Sc. degree from the University of Santa Cruz do Sul (UNISC/2010), and M.Sc. from the Federal University of Rio Grande do Sul (UFRGS/2014), both in Computer Science.

Matthew Luckie received his Ph.D. degree from the University of Waikato, Hamilton, New Zealand in 2006. He is a senior lecturer in the Computer Science Department at Waikato. Prior to that, he was a research scientist (2014–2015) and a postdoc (2012–2014) at CAIDA, UC San Diego, and a lecturer (2006–2010)/senior lecturer (2011) at the University of Waikato. His research interest includes the economic relationships between ASes, inferring the router-level topology, and development of distributable software for collecting IP-level data.

Bradley Huffaker received his B.S. and M.S. degrees in computer science from University of California, San Diego, California, United States, in 2000. He has been at UCSD/CAIDA since 1998 and he is currently technical lead focusing on efforts to develop analytical techniques suitable for gaining insight on the configuration, evolution, and occurrence of network events in large network topologies.

Kimberly Claffy received the B.S. degree in symbolic systems from Stanford, Stanford, California, United States, in 1989 and M.S. degree in computer science and engineering from University of California, San Diego, California, United States, in 1991. Then she received the Ph.D. degree in computer science and engineering from University of California, San Diego, California, United States, in 1994. She is founder and director of the Center for Applied Internet Data Analysis (CAIDA), a resident research scientist of the San Diego Supercomputer Center at UC, San Diego, and an Adjunct Professor in the Computer Science and Engineering Department at UC, San Diego. Her research interests span Internet topology, routing, security, economics, future Internet architectures, and policy. She leads CAIDA research and infrastructure efforts in Internet cartography, aimed at characterizing the changing nature of the Internet's topology, routing and traffic dynamics, and investigating the implications of these changes on network science, architecture, infrastructure security and stability, and public policy. Dr. Claffy's awards and honors include the Jonathan B. Postel Service Award in 2017 and IEEE Internet Award in 2015.

Marinho Barcellos joined in October 2019 the School of Computer and Mathematical Sciences at University of Waikato as a Senior Lecturer. Between 2010 and 2019 he worked as an Associate Professor at INF/UFRGS, and prior to that, at Unisinos (1993–2008) and PUC-RS (2008–2009), all in Brazil. He was a holder of a distinguished researcher CNPq grant (Level 1D). As for public service, he is a currently member of the ACM SIGCOMM executive committee (helping with diversity and outreach), a co-chair of its CARES committee (against harassment), and a member of ACM CoNEXT steering committee. In 2019 he helped with ACM LANCOMM (general co-chair), PAM (program co-chair) and ACM CoNEXT (publications co-chair).