Detection, Classification, and Analysis of Inter-Domain Traffic with Spoofed Source IP Addresses

Franziska Lichtblau
TU Berlin
franziska@inet.tu-berlin.de

Florian Streibelt
TU Berlin
florian@inet.tu-berlin.de

Thorben Krüger
TU Berlin
thorben@inet.tu-berlin.de

Philipp Richter
TU Berlin
prichter@inet.tu-berlin.de

Anja Feldmann
TU Berlin
anja@inet.tu-berlin.de

ABSTRACT

IP traffic with forged source addresses (i.e., spoofed traffic) enables a series of threats ranging from the impersonation of remote hosts to massive denial-of-service attacks. Consequently, IP address spoofing received considerable attention with efforts to either suppress spoofing, to mitigate its consequences, or to actively measure the ability to spoof in individual networks. However, as of today, we still lack a comprehensive understanding both of the prevalence and the characteristics of spoofed traffic "in the wild" as well as of the networks that inject spoofed traffic into the Internet.

In this paper, we propose and evaluate a method to passively detect spoofed packets in traffic exchanged between networks in the inter-domain Internet. Our detection mechanism identifies both source IP addresses that should never be visible in the inter-domain Internet (i.e., unrouted and bogon sources) as well as source addresses that should not be sourced by individual networks, as inferred from BGP routing information. We apply our method to classify the traffic exchanged between more than 700 networks at a large European IXP. We find that the majority of connected networks do not, or not consistently, filter their outgoing traffic. Filtering strategies and contributions of spoofed traffic vary heavily across networks of different types and sizes. Finally, we study qualitative characteristics of spoofed traffic, regarding both application popularity as well as structural properties of addresses. Combining our observations, we identify and study dominant attack patterns.

CCS CONCEPTS

• **Networks** → **Network measurement**; **Network security**;

KEYWORDS

IP spoofing, Inter-domain traffic, Denial-of-service, Network filtering

IMC'17, November 2017, London, UK

ACM ISBN 978-1-4503-5118-8/17/11.
https://doi.org/10.1145/3131365.3131367

ACM Reference Format:
Franziska Lichtblau, Florian Streibelt, Thorben Krüger, Philipp Richter, and Anja Feldmann. 2017. Detection, Classification, and Analysis of Inter-Domain Traffic with Spoofed Source IP Addresses. In *Proceedings of ACM Internet Measurements Conference (IMC'17).* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3131365.3131367

1 INTRODUCTION

The Internet Protocol (IP) provides a unified and simple abstraction for communication over the Internet. It identifies hosts by their IP addresses, allowing for data exchanges across heterogeneous networks. While the simplicity of the Internet Protocol has proven immensely powerful it comes with inherent limitations, such as the lack of packet-level authenticity. Routers perform only a lookup for the destination address of incoming packets, the authenticity of source IP addresses of packets is not validated on the path between sender and receiver.

The resulting ability to forge the source IP address of a packet (i.e., *spoofing*) enables a series of cybersecurity threats, ranging from the impersonation of remote hosts to massive denial-of-service Attacks, causing major disruptions of Internet services [48]. In response, the IETF developed best practices for ingress traffic filtering at autonomous system (AS) borders [23]. The spoofing problem also received considerable attention from the research community with systems and architectures that have the potential to either limit or prevent spoofing in the Internet (e.g., [6, 24, 32]). However, these mitigation approaches have not succeeded in eliminating spoofing in production environments: Attacks involving spoofed source IP addresses remain widespread [17, 37].

The measurement community has been very successful in detecting the *ability* to spoof in individual networks using active measurements, i.e., by explicitly crafting packets with spoofed source addresses and measuring the receipt or non-receipt of such packets [10, 11]. While active measurements to assess "spoofability" are indispensable resources to track the deployment of ingress filtering in the Internet, they yield no insight into *if* and *how* the ability to spoof packets is exploited in the Internet. As of today, we still lack a detailed understanding of how to detect spoofed traffic "in the wild". Consequently, little is known about the quantitative and qualitative properties of spoofed traffic, nor about the types of networks that source spoofed traffic into the Internet. The absence of well-tested techniques to detect such traffic as well as detailed measurements documenting the dominant characteristics of spoofed traffic are a major obstacle both for networks operators and for designers of

operational systems, who have to rely on best guesses on how to identify such traffic and protect their systems against it.

We, in this paper, present a first-of-its-kind study that focuses on passive detection and analysis of spoofed traffic as observed in the Internet. To accomplish this, we first develop and evaluate tools that enable us to detect spoofed traffic in network traces. We then apply our detection method to classify the traffic exchanged between some 700 networks that peer at a major European IXP. Our method, combined with our vantage point, allows us to provide unprecedented insights into traffic and network characteristics inherent to spoofing in today's Internet. Our main contributions can be summarized as follows:

(i) We develop a new approach to passively detect packets with spoofed IP addresses in inter-domain traffic. Our approach identifies and leverages sets of valid IP address ranges for individual ASes, derived from transitive AS relationships in BGP data. It allows us to filter out spoofed traffic both with unrouted as well as routed source addresses. We compare and evaluate different techniques to generate AS-specific lists of valid address space and minimize false positive inferences.

(ii) We apply our detection method to classify the traffic exchanged between some 700 networks peering at a major European IXP and provide detailed statistics regarding which networks deploy what kind of address filtering in practice. We then quantify the extent to which individual networks contribute to the different types of spoofed traffic at our vantage point, taking their individual business types and overall traffic shares into account.

(iii) We present a first in-depth analysis of the qualitative characteristics of spoofed traffic exchanged in the inter-domain Internet. We study traffic characteristics involving both time-of-the-day effects, spoofed applications, as well as the structure of source and destination addresses. Combining our observations, we identify and study dominant attack patterns.

Our tools and findings have a number of implications for the networking and research community. Our evaluation of BGP-based spoofing detection yields important considerations and pitfalls for network operators that plan to deploy filtering based on BGP data. Our empirical analysis of the deployment of different filtering techniques as well as spoofing contribution by individual networks can assist network operators when deciding with which networks to peer and under which conditions. Our study of the characteristics of spoofed traffic provides hard-to-get insights that are imperative resources for designing and deploying effective anti-spoofing mechanisms and approaches. We note, however, that our approach is only applicable to inter-domain traffic and, hence, only partially illuminates Internet-wide spoofing. In particular, our approach can not detect "same subnet spoofing", i.e., cases where the spoofed IP addresses belong to the as-legitimate-identified address space of the network sending the traffic. In this work, we consider IPv4 traffic exclusively, as native IPv6 traffic still ranges below 3% at our vantage point.

The remainder of this paper is structured as follows: In Section 2 we introduce spoofing and provide up-to-date practical insights on spoofing and the resulting challenges from a survey we conducted among network operators. In Section 3 we introduce our techniques to infer valid address ranges for individual networks and to detect spoofed traffic. We apply and evaluate our methodology in Section 4, and study network-specific spoofing contributions in Section 5. We assess characteristics of spoofed traffic in Section 6 and highlight attack patterns in Section 7.

2 THE UNSOLVED SPOOFING PROBLEM

The lack of packet-level authenticity of the IP protocol allows for forgery of source IP addresses. This is leveraged by a multitude of attacks that have a vast impact on today's Internet. Despite many ongoing efforts within the research and operations communities to combat IP spoofing, the problem has remained unsolved for more than 30 years [40]. In this section, we provide necessary background on IP address spoofing. We first introduce two common types of attacks involving spoofed source addresses and discuss network filtering practices. We then provide up-to-date perspectives on spoofing and filtering, derived from a network operator survey we conducted. We conclude with a discussion of related work.

2.1 Spoofing Attacks and Network Filtering

We next introduce the two most prominent types of denial-of-service attacks that are enabled by spoofed traffic. We then discuss filtering options that operators have to prevent such attacks.

Flooding Attacks: The attacker overwhelms the victim with packets, either to exhaust the victim's bandwidth resources, or to disrupt the victim's operating system. Here, source IP address forging allows to conceal the true origin(s) of the sender(s) and can cause massive depletion of the victims' operating system resources, e.g., by flooding with TCP SYN packets from a multitude of source IP addresses, exhausting the state of the victim's TCP stack to the point of disrupting all its network communication [22]. More importantly, randomly spoofing source addresses from a large address range typically makes it impractical, if not impossible, for the victim to filter the offending traffic based on address information alone.

Amplification Attacks: Here, the attackers send crafted packets carrying the source IP address of the intended victim to servers (*amplifiers*) that run a service susceptible to amplification (e.g., NTP or DNS [48]). The servers, in turn, send replies to the victim's IP address that can be orders of magnitude larger than the original requests. This leads to the victim being flooded with a vast amount of unsolicited traffic, potentially disrupting its operation. The ability to forge *specific* IP addresses is essential for this type of attack.

Network Filtering: The decentralized nature of the Internet makes the spoofing problem difficult to address, since there are few topological locations where packet-level sender authenticity can be verified in a straight-forward manner. While it is virtually possible to filter traffic at any given router in the network, the most commonly deployed strategy to prevent spoofing relies on traffic filtering at the AS boundary. In practice, this is achieved by deploying ACLs (Access Control Lists) that only allow traffic with source IP addresses covered by specified prefixes to enter the network. ACLs can be whitelists (i.e., specify a list of allowed prefixes) or blacklists (i.e., specify a list of forbidden prefixes). We synonymously refer to these ACLs as filter lists. Filtering at the AS boundary can be implemented at the *ingress* or the *egress*.

Traffic is most commonly filtered at the ingress, referring to the border router where traffic from other networks (peers) enters the network. Here, the border router maintains a continuously updated list of all prefixes for which it is allowed to accept traffic on a certain interface, from a certain peer. Traffic with IP addresses that are not covered by these prefixes will be dropped before entering the network. Leveraging this strategy to eliminate IP spoofing is documented in detail by Best Current Practices (BCP) documents 38[23] and 84[8]. It is also possible to deploy filtering at the egress where traffic leaves the network, here the same concepts apply as for ingress filtering.

Both strategies rely on prefix lists that must be generated and constantly maintained. In the case of negative filters which mostly refer to a small set of static prefixes (e.g., private address space [43]) the task is trivial since such filters can be statically configured. For fine-grained filtering of valid and routed prefixes that belong to the network and its peers, however, a comprehensive overview of the peering topology as well as constant maintenance are necessary. As of today, no reliable general mechanism for automatically creating these kinds of filter lists exist.

2.2 Spoofing and Filtering in Practice

To understand both the challenges that network operators face when it comes to the deployment of network filtering and the direct impact of source IP address spoofing on their operation, we conducted a survey in early 2017. We circulated a questionnaire across 12 network operator mailing lists, including NANOG [2], RIPE [5], and several local network operator groups. We received answers from 84 networks, covering all geographic regions and a wide range of network types, including transit ISPs, end-user ISPs, hosters, and content providers. While we do not claim our data to be an unbiased sample, we are able to identify some common challenges that many operators face as of today.

Spoofing Impact: Over 70% of the participants confirmed having suffered from network attacks related to IP source address spoofing that could have been prevented by a broader deployment of consistent filtering mechanisms. Furthermore, 50% of the networks did actively send complaints to peers that did not filter correctly. On the other hand, 24% of the participating operators mentioned that they do not check the validity of source IP addresses at all. Hence, while the topic of spoofing and ways to limit its impact are known, it remains an unsolved problem within the operator community, where it consumes significant human and technology resources.

Filtering Strategies: We inquired about ingress as well as egress filtering. Overall, the replies indicate that network ingress filtering is more commonly deployed than egress filtering, which is due to the fact that traffic that is dropped at the network entry does not need to be transported any further. Up to 70% of the respondents filter well-known ranges that should not be routed in the inter-domain Internet, e.g, RFC1918, and other reserved space. Only 20% apply customer-specific filters at the ingress and 7% indicated to not filter ingress traffic at all. Looking at the egress, about 50% of the participants have customer AS-specific egress filters, 24% do not apply any egress filters, and some 26% only filter non-routable space. Regarding traffic originating within their own network, 65% of the operators indicated that they filter their traffic before it can reach the egress router. Generally our survey indicates that while many networks filter static non-routable prefixes, only about half of them deploy peer-specific filters.

Filtering Challenges and Incentives: The most commonly mentioned reason for *not* filtering traffic is the inherent possibility to drop legitimate traffic from (paying) customers. A vast majority of participants indicate that the required planning, knowledge, coordination, and time needed to maintain accurate and up-to-date peer-specific filter lists is out of reach for them. A commonly mentioned solution is RPF (Reverse Path Filtering, i.e., only accepting traffic from routes that the customer advertises to the provider [8]), but its strict implementation becomes a problem in the case of asymmetric routing, particularly in multi-homed networks. Additionally, participants mentioned that their network equipment often lacks proper RPF support. Apart from technical limitations, some respondents mentioned that the effort of running a "clean" network does not result in direct economic benefit for them and is, therefore, a low priority. Many respondents explicitly state that spoofed traffic only accounts for a small fraction of traffic in terms of total volume. Hence, spoofing prevention is less of a concern when it comes to the actual cost of transporting traffic. For most of our respondents, the motivation to run a "clean" network is to protect their peers and take part in the global struggle against spoofing, albeit reducing abuse complaints.

Given the limited opportunities to get in touch with network operators, our sample is unavoidably biased by operators who already took some measures to deploy network filtering. We hence presume that the number of networks that do not comply with best common filtering practices "in the wild" is much larger, which we study empirically in Section 5.

2.3 Related Work

The IETF publishes several best practices documenting how to prevent inter-domain spoofing with ingress filtering, most importantly BCP38 [23] and BCP84 [8]. As already detailed, there are various reasons why operators decide to not apply strict filtering. As a result, initiatives such as the MANRS project [1] emerged, providing additional documentation and guidance on how to deploy strict filtering in operational networks. Spoofing also received considerable attention from the research community, with approaches to prevent spoofing or to mitigate its impact, measurement studies documenting attacks with spoofed IP addresses, and measurements to detect the ability to spoof in networks.

Spoofing Mitigation: Several systems and architectures have been proposed to either reduce spoofability or to prevent it altogether within networks or at the network boundaries [6, 24, 31–33, 38, 50, 54, 56]. Other studies suggest improvements to harden protocols to alleviate the impact of spoofed packets. Rossow identified and studied protocols prone to amplification attacks [48]. Kührer et al. suggest approaches that help to reduce the number NTP servers vulnerable to amplification by 92% [29]. Zhu et al. [57] suggest connection-oriented DNS to prevent the exploitation of open DNS resolvers, e.g., for amplification attacks [28].

Spoofing Effects: Several studies show the extent and impact of attacks involving spoofed source addresses. In an early work, Hussain et al. [27] developed a framework for detecting and classifying

DDoS attacks involving spoofed source addresses. In 2014, Czyz et al. studied NTP amplification attacks which were performed using UDP packets with spoofed source addresses, finding that 85% of DDoS attacks exceeding 100 Gbps in 2014 were using NTP amplification [18]. In 2015, Miao et al. found that 67% of TCP SYN flooding attacks at a globally distributed cloud provider involve spoofed addresses [37]. Moura et al. studied massive attacks on the root DNS server, finding that spoofed source addresses significantly contributed [41]. Luckie et al. demonstrated in 2015 that spoofing can also be used for attacks on TCP sessions, finding that 38.4% of web servers and middleboxes were vulnerable to a TCP reset attack. Kührer et al. found that, in contrast to common belief, also TCP-based protocols can be used for amplification attacks, finding amplification factors of 50x and higher [30].

Spoofing Detection: Some works actively detect the ability to spoof in certain networks. The Spoofer project, initiated by Beverly et al. see [10, 11], now maintained by CAIDA [14], measures spoofability within networks by actively sending packets with forged source addresses to a measurement server. Their data, as of 2017, shows that spoofing was possible in more than 34% of the 2.5K tested networks, and partially possible in another 17% [14]. Kührer et al. detected spoofed traffic remotely, utilizing DNS resolvers and found that more than 2.7K ASes do not perform egress filtering [29]. Lone et al. propose a method that inspects IP addresses in traceroute measurements to detect the ability to spoof in networks [34]. Some work exists that identifies spoofed traffic passively, based on address characteristics. Moore et al. were the first to propose source address uniformity as a detection mechanism [39]. Yao et al. use passive measurements to investigate backscatter of on-path network equipment for unwanted traffic [55]. Dainotti et al. detected unrouted source addresses in passive traces [19, 20]. Chen et al. and Barford et al. studied characteristics of malicious source addresses, finding that unrouted source addresses contribute more than 7% of attack traffic [9, 15].

Our study contributes to the body of work in this challenging field. We present a new and complementary approach that allows for passive detection of spoofed traffic. Our analysis provides profound insights into both filtering setups deployed by networks in the wild, quantifies the contribution of individual networks, and studies dominant characteristics of real-world spoofed traffic.

3 METHODOLOGY

In this section, we describe our methodology to passively detect spoofed packets in inter-domain traffic. In contrast to active measurements using deliberately crafted packets, our method does not rely on any explicit information about a given packet beyond its source IP address to detect spoofing. Our approach classifies source IP addresses of packets as either *legitimate* or *illegitimate*. However, not all traffic with illegitimate source IP addresses is necessarily a case of spoofing. We argue for the following distinction among packets with illegitimate source addresses:

Packets with Stray source IP addresses: These are packets with source IP addresses that are the genuine addresses of some interface of the host sending the packet. Yet, packets with such source addresses should either not be forwarded in the inter-domain Internet at all, or not be sourced by a particular AS. The former includes *bogon* IP addresses, e.g., RFC1918. The latter includes traffic with valid routable source IP addresses that we observe on inter-domain links that should not carry them (e.g., routers sending out TTL exceeded over their default route). Typically, stray source IP addresses are the result of misconfiguration without malicious intent.

Packets with Spoofed source IP addresses: In this case the source address is unrelated to any of the genuine IPs of the host sending the packet. Such packets are typically crafted with the intent of misrepresenting the source IP address in a packet to either conceal the identity of the sender or to impersonate another host.

Our goal is to identify traffic with spoofed source IP addresses and to distinguish it from traffic with stray source IP addresses. First, however, we study the categories of IP source addresses that are relevant for our detection method.

3.1 Address Space Considerations

To bootstrap our classification approach, we first partition the IPv4 address space into four categories, shown in Figure 1a: Address space that should not be routed in the inter-domain Internet at all, i.e., reserved ranges, which we refer to as "bogon", and address ranges that are routable, yet we do not find them announced in the global routing table, which we refer to as "unrouted". These source ranges are AS agnostic in the sense that no network should source traffic from these ranges into the inter-domain Internet. The other category includes the IP address space routed in the inter-domain Internet. Here, we distinguish between "invalid" and "valid" address space on a per AS basis.

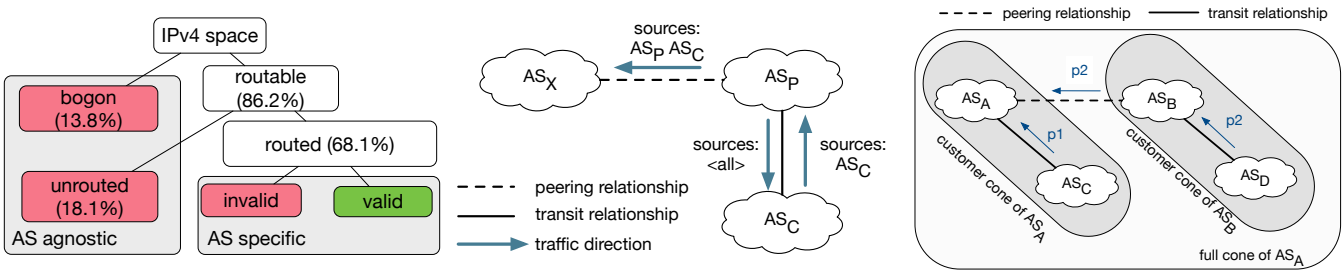
Bogon Source Addresses: The bogon space captures the address space that is not intended to be used in the public Internet. Bogon source ranges are defined in, e.g., RFC1918 [43], RFC5738 [16], and RFC6598 [53]. They include private address ranges as well as multicast and future use.

Unrouted Source Addresses: These addresses *are* part of the routable space, but are not covered by a BGP announcement in the global routing table. We later use extensive BGP datasets to compile a list of currently routed IPv4 prefixes and we consider every address that is not covered by any prefix as unrouted.

Invalid Source Addresses: Naturally, packets with a given IP source address should only be originated from the AS that also announces the prefix covering that address. In accordance with best current practices, they should furthermore only be forwarded by ASes that are in an upstream or peering relation to the announcing AS[1] [8]. We use this observation as a criterion to identify *valid* source ASes for traffic with given source IP addresses. The complexity of determining whether an AS is a valid source for a given IP address depends on its distance from the origin AS in terms of BGP AS distance. In the simplest case, if an AS is a *stub AS*, i.e., not providing transit to any other AS, it is only a valid source for its own prefixes. For *transit ASes*, i.e., networks that forward traffic on behalf of other networks, the situation becomes more complex.

In Figure 1b, two networks engage in a *transit* relationship, customer AS_C pays provider AS_P to *(a)* forward traffic it receives from

[1] Some mechanisms take advantage of the fact that this is not strictly realized in the current Internet, e.g., Mobile IP with triangle routing. However, Mobile IP acknowledges this problem and proposes direct routing as an alternative [42].



(a) Categories of IPv4 Addresses relevant for passive spoofing classification.

(b) Traffic patterns and source addresses in peering and transit AS relationships.

(c) Full Cone: AS_A can forward AS_B's traffic to AS_C, contrary to customer cone.

Figure 1: Inference of valid address space per AS.

the customer to the rest of the Internet, but also *(b)* to forward traffic from the rest of the Internet towards the customers' routes. Thus, an AS that provides transit typically either offers a full BGP table to its customers or a default route, and is thereby allowed to source the whole routed address space on the links to its customers. If two ASes engage in a *peering* relationship, e.g., AS_P and AS_X in Figure 1b, they should only exchange traffic between each other, in particular traffic originating in their own network or in one of their customers. Thus, for the link between AS_P and AS_X, valid sources for AS_P are source IP addresses from AS_P and AS_C. Hence, address range validity for an AS depends both on its position in the AS-level topology, as well as on the link on which we monitor traffic. Based on the above discussion we will consider any traffic with an invalid source address that is forwarded by an AS to be potentially spoofed.

3.2 Inferring Valid IP Space per AS

Our above discussion underlines the need to consider inter-domain information to identify valid source address ranges. We next introduce three approaches for inferring valid IP address space on a per AS basis, ranging from conservative to liberal in terms of the amount of valid IP space per AS.

Naive Approach: As a baseline approach we consider ASes as valid sources for traffic from a given prefix, if we observe the AS on the path of a route announcement of the respective prefix.[2] This information is contained in the BGP AS-path (i.e., the list of all ASes that the announcement has traversed). The naive approach does not account for asymmetric routing or selective announcements; i.e., cases in which an AS does not announce all of its prefixes to all neighbors, but still sends traffic from any of these prefixes to any of them. In such cases, the naive approach tags packets of the partially announced or propagated source prefixes as invalid.

CAIDA Customer Cone: Luckie et al. [36] suggested to use the *CAIDA Customer Cone* [35] for identifying spoofed traffic. The customer cone of an AS is the set of ASes that an AS can reach using provider-customer links. Thus, if *AS A* is the origin of a prefix, then all ASes that include *AS A* in their customer cones may source traffic with source IPs from this prefix. This approach focuses on customer-provider relationships. As such, it intentionally does not take equitable peering relationships into account.

Full Cone: The previous two approaches have the potential to misclassify traffic as invalid, either due to asymmetric routing or due to traffic carried over peering links which the customer cone (intentionally) does not cover. Since we strive to minimize false positive classifications, we develop the *Full Cone*, where we *intentionally sacrifice specificity* compared to the other approaches, by not distinguishing between peering/sibling, customer-provider and provider-customer links. Rather, whenever we see two neighboring ASes on an AS path, we presume a directed link between the two, where the left AS is considered upstream of the right AS. On the resulting directed AS graph (that may indeed contain loops) we calculate for each AS the *transitive closure* containing all its children. Thus, if *AS A* is the origin of a prefix then all ASes that include *AS A* in their transitive closure may source traffic with source IP addresses from this prefix. The Full Cone is the least specific of our approaches, but has the advantage of accounting for peering relationships as well as atypical traffic patterns. Figure 1c highlights the potential benefits of this approach when it comes to minimizing false positive classifications: Here, AS_A and AS_B peer with each other. AS_C is a customer of AS_A and AS_D is a customer of AS_B. As such AS_D/AS_C is in the CAIDA Customer Cone of AS_B/AS_A, respectively. However, these disjoint Customer Cones do not capture the peering relationship. As a consequence, traffic with source IPs in prefix p_2 by AS_D would not be considered valid at AS_A.

Multi-AS Organizations: Our three approaches rely on the existence of visible BGP links. In the case of organizations that use multiple AS numbers, *Multi-AS organizations* [12], peering links between their individual ASes are not necessarily exposed in the global routing table. For the goal of this work, identifying intentionally spoofed traffic, we allow for bidirectional traffic exchange between ASes belonging to the same organization. To identify ASes belonging to the same organization, we rely on CAIDA's *AS to Organization* [26] dataset. This dataset links ASes to organizations based on the available WHOIS information (e.g., email and physical address, name, and contact information). We extract sets of ASes belonging to the same organization, and add a full mesh of links between all ASes within each set. The joint cones and IP address space of each organization is now shared with each constituent AS belonging to the same set, regardless of whether this relationship

[2] This reasoning is also in line with "reverse path forwarding", requiring the reverse route to have been learned from a peer before allowing traffic to be forwarded to it, see BCP84 [8].

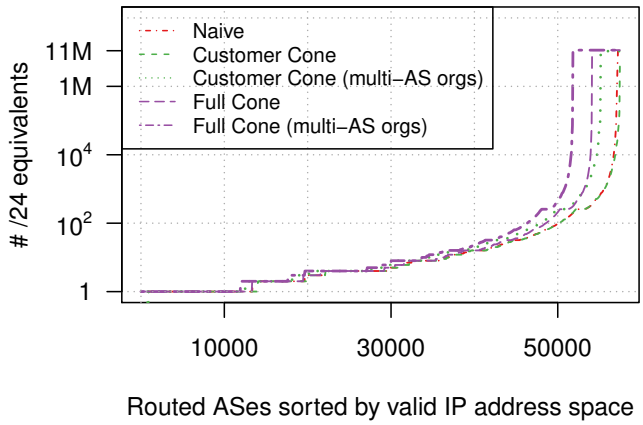


Figure 2: Routed ASes sorted by the size of their valid address space based on *Customer Cone* and *Full Cone* inference methods, either with or without considering multi-AS organizations. *Naive* is included as baseline.

is reflected in BGP or not. This way, traffic forwarded on behalf of an AS of the same organization is not considered invalid.

3.3 Routing Datasets

To determine bogon, unrouted, as well as valid address space for each AS, we rely on the following datasets:

Bogon Lists: We use a list of bogon prefixes as provided by Team Cymru [51], which are widely used by operators for egress filtering. The resulting bogon list contains 14 non-overlapping prefixes corresponding to 218K /24 equivalents.

BGP Datasets: To determine the routable address space as well as to construct the network-specific list of valid address space we rely *(i)* on publicly available BGP datasets as well as *(ii)* on vantage point-specific BGP data. Our measurement period spans 4 weeks from February 5th, 2017 to March 6th, 2017. In particular, we use BGP data from all route collectors from RIPE RIS [47] and RouteViews [52] that have data available for our measurement period (18 out of 21 collectors for RIPE, 16 collectors for RouteViews). RIPE and RouteViews offer snapshots (every 8 hours for RIPE and every 2 hours for RouteViews) of the collector's routing table, as well as all BGP updates that the collector receives from its peers. Note that ASes commonly announce changing sets of prefixes with varying aggregation levels at multiple locations to different networks. To acquire an as-complete-as-possible picture of routed prefixes and of the AS graph, we consider *all* table dumps and update messages within our time period. We disregard announcements for prefixes more specific than /24 and less specific than /8. The latter usually indicates misconfiguration and neither is commonly routed [21]. In total, our announcements cover 11.65M routed /24 equivalents. We extend our BGP datasets with vantage point-specific BGP data from the route server [46] of a major IXP, which will be our vantage point to study spoofed traffic (Section 4).

3.4 Comparison of the Three Approaches

Figure 2 shows for each of our approaches the size of the valid IP address space (in /24 equivalents) for each routed AS. Here, we sort the ASes in increasing order according to the size of their valid address space.[3] Furthermore, we show our cone methods both with and without adjustments for multi-AS organizations. We find that, unsurprisingly, all approaches agree on about 12K of the smallest stub ASes. For the remaining ASes, the adjustments for multi-AS organizations consistently cover more address space than the plain, non-adjusted approaches. For the latter, the covered address space only significantly diverges for top 14K ASes. The Full Cone, as expected, yields larger valid address spaces, since it takes any transitive AS relationship into account. Here, we see that for the top 14K ASes the size of their valid address space grows considerably and an upwards of 5K ASes are a valid source for the entire routed address space, roughly 11M /24s. In addition, we also confirmed that the address spaces per AS for the Naive approach as well as for the Customer Cone are fully contained within the Full Cone. Combined with the consistently higher coverage when including adjustments for multi-AS organizations, the Full Cone is the preferred candidate in our endeavor to identify spoofed traffic with an emphasis on minimizing false positive detections.

4 SPOOFING DETECTION IN PRACTICE

We next apply our method to classify the traffic exchanged between some 700 networks at a major European IXP. While this vantage point provides us with a unique opportunity to study spoofing at scale we point out that our approach is not limited to IXPs: It is applicable for any vantage point that captures inter-domain traffic.

4.1 Vantage Point and Traffic Dataset

We use four weeks of continuous traffic traces captured in February 2017 at a major European IXP. IXPs provide a layer-2 switching infrastructure to participating networks, called *members* in the following. Members connect with their border routers to the switching fabric, establish BGP sessions with other members[4] and exchange traffic with each other. At the time of this measurement, the IXP had 727 members that exchanged about 230PB traffic on a weekly basis with peak traffic rates exceeding 5 Tb/s. Our traces consist of IPFIX flow summaries which are collected using a random 1 out of 10K sampling of all packets crossing the IXP's switching fabric. The available flow information includes the IP and transport layer headers, as well as flow summaries with packet and byte counts. Thus, at this vantage point, we capture the inter-domain traffic right at the border between ASes.

4.2 Classification Pipeline

Our passive spoofing detection mechanism classifies each flow based on its source IP address into either Bogon, Unrouted, Invalid, or valid, see Figure 3. Hereby, Bogon and Unrouted refer to the AS agnostic address ranges and Invalid to the AS specific address ranges, recall Section 3.1. valid contains all other flows and is not further considered. Our classification is strictly sequential, see Figure 3. Once we match a source IP address into a class we stop.

[3] Note that this figure shows the distribution of valid ranges per AS for each approach individually and does hence not allow for comparison of individual ASes.

[4] This IXP also provides a route server to its members. Members can opt to establish a single BGP session with the route server to immediately engage in *multilateral* peering with a large number of other members [46]. We, in this paper, use BGP snapshots from the IXPs route server in addition to publicly available BGP data.

	Bogon		Unrouted		Invalid FULL		Invalid NAIVE		Invalid CC	
members	525	(72.0%)	378	(52.0%)	393	(54.06%)	611	(84.04%)	602	(82.81%)
bytes	31.63T	(0.003%)	38.29T	(0.004%)	92.65T	(0.0099%)	10.08P	(1.1%)	1.72P	(0.19%)
packets	304.82G	(0.02%)	217.59G	(0.02%)	387.23G	(0.03%)	17.20T	(1.29%)	4.05T	(0.3%)

Table 1: Contributions to each class for our inference approaches (Traffic scaled to account for sampling).

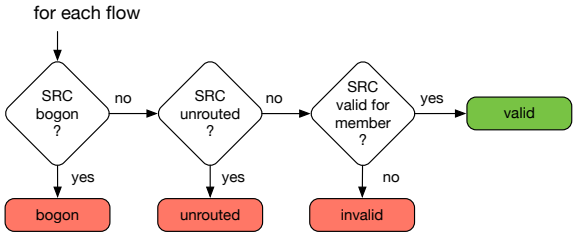


Figure 3: Applying our methodology to dissect traffic.

Thus, all classes are mutually exclusive. We use the following flow features: source IP address, associated origin AS, and via which IXP member the flow entered the IXP. First, we match the source IP address against the bogon list. Next, we match the source IP address against the routed address space. The following step takes the member AS into account. If we find that the member is not a valid source for this source IP address, we classify the flow as Invalid. To determine this, we check if the IP address is part of the legitimate address space of the member AS, according to each of our three approaches, see Section 3.2. This results in three different sets of invalid traffic, namely, Invalid NAIVE, Invalid CC, and Invalid FULL.

4.3 Classification Results

The results of applying the above methodology to four weeks of traffic are summarized in Table 1. Here, we show both absolute and relative traffic contribution for each class as well as the number of members that contribute traffic to each class.

Bogon and Unrouted: We observe that more than 72% of the member networks send packets with bogon source IP addresses and 52% send packets with unrouted source addresses. A striking observation, suggesting that the **majority of members do not, or not consistently, filter their outbound traffic**. When taking the relative contribution in terms of packets and bytes into account, however, we see that the share is comparably low, with Unrouted and Bogon traffic accounting for about 0.02% of the overall traffic. Nevertheless, these traffic contributions sum up to tens of TBs over the course of four weeks. Comparing the contribution of Bogon to Unrouted, we see that Bogon has more contributing members while Unrouted has higher traffic volumes though less packets. One possible explanation for packets in Bogon are devices behind misconfigured network address translation devices (NATs). Packets in Unrouted, on the other hand, are more likely to be caused by intentional source IP address forgery. Apparently, NAT misconfigurations are more common (when seen on a per-network granularity) when compared to source IP address forgery. We point out, however, that Unrouted traffic contributes more in terms of absolute bytes, suggesting that while fewer networks emit such traffic, they typically emit larger quantities, compared to Bogon.

Invalid: The three right columns of Table 1 show the number of members and respective traffic volume classified as Invalid for our three approaches (recall Section 3). Here, we observe significant differences across the three approaches. The conservative Invalid FULL, naturally, classifies the smallest portion of traffic as Invalid. Still, more than half of the members contribute traffic to this class. Invalid NAIVE and Invalid CC identify a significantly larger share of traffic, well exceeding 1% and 0.1% respectively of the total traffic, and including about 80% of members. These observations are in line with the different cone sizes as explored in Section 3.4, i.e., the Naive approach and the Invalid CC approach allow less valid address space per AS and hence classify more traffic as Invalid. We observe that the number of members that contribute to Invalid NAIVE and Invalid CC well exceed the number of members that contribute to our classes Bogon and Unrouted, which are less prone to false positives as they are AS agnostic.

Impact of Multi-AS Organizations: The results shown in Table 1 allow bidirectional traffic flow across multi-AS organizations, irrespective of the existence or inferred business type of BGP peerings (recall Section 3.2). Allowing such traffic has a different impact on our individual approaches. Allowing inter-organization traffic reduces invalid traffic in Invalid FULL by some 15%, but by almost 85% in the case of Invalid CC. The vast reduction in the case of Invalid CC is due to few heavy traffic-carrying members and closer inspection shows that these members indeed have visible AS links and are thus contained in the Invalid FULL cone, which does not differentiate between different business relationships. Invalid CC only allows customer-provider relationships and hence intentionally discards these relationships. Our results suggest that the customer cone is a promising approach, when refined to take complex AS relationships such as multi-AS organizations into account.

We, in this work, strive to minimize *false positive* classifications. We hence proceed with our analysis with the Full Cone approach, i.e., from now on we will only study Invalid FULL traffic and refer to it as Invalid.

4.4 Hunting False Positives

Even our most conservative approach, Invalid FULL, includes false positives, i.e., traffic from source addresses that a member can legitimately source, yet we classify it as Invalid, caused by missing AS relationships. Missing AS relationships can be caused by *(a)* the inherently limited coverage of the AS graph in the available BGP data [25] and *(b)* inter-AS connectivity that is not exposed in the global routing table (e.g., tunnels). To identify traffic that we possibly misclassify as Invalid due to missing AS relationships, we focus on those ASes for which Invalid accounts for a significant share of their overall traffic. Figure 4 shows a CCDF of the fraction of the Bogon, Unrouted and Invalid traffic share of the overall traffic for each member. We note that the largest contribution of any member to Bogon is about 10% and to Unrouted about 9%.

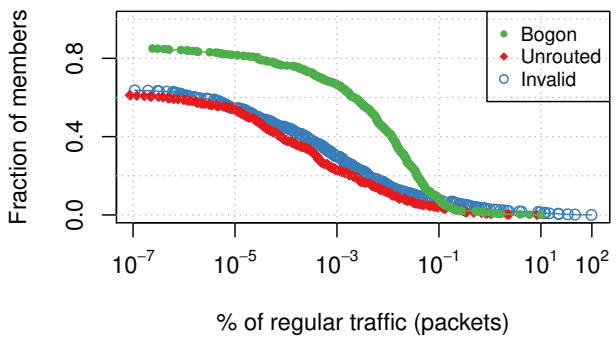


Figure 4: Fraction of Bogon, Unrouted and Invalid of total traffic per IXP member AS.

For Invalid, however, we find some few members who contribute close to 100% of their entire traffic to Invalid.

To asses whether we misattribute traffic of these members to be Invalid, we take a closer look at the top 40 member ASes as shown in the CCDF. For these, we generate per-member statistics containing the origin ASes of the source and destination IP addresses in question. Next, we check the databases of the Routing Internet Registries (WHOIS) for missing AS relationships between the member AS sending the traffic, the origin AS of the source and destination IP addresses, and the member AS receiving the traffic. In particular, we study import and export ACLs that some ASes publish to indicate routing policies. We also leverage information from looking glasses located inside some of these ASes.

Missing AS Links: We identified 15 missing links using WHOIS records, i.e., by matching company names or contact points that are not covered by the AS-to-organization dataset we use, or by matching import/export ACLs for direct peerings. In addition, we find one additional AS relationship based on looking glass information. We identify one instance where two closely related organizations that operate shared network infrastructure exchange internal traffic between parts of their networks via the IXP. Additionally, we encounter several instances where WHOIS data shows that one AS is (or was) an upstream provider, but we do not see evidence in the BGP data at the time we captured the traffic. We currently do not investigate archived BGP data and consider this as future work together with incorporating automated parsing and evaluation of the import and export ACLs to enrich the available BGP data collected.

Uncommon Setups: We also found instances of uncommon routing setups that are not BCP38 compliant. In two cases a customer with multiple upstream providers uses provider-assigned address space from one provider to send traffic via the other provider to the Internet. Analysis of the WHOIS entries reveals that, while the ISP only announces a single covering prefix, an entry in the WHOIS database exists for both customer prefixes naming the customers. In another case we find a cloud-based startup that uses uncommon traffic engineering by tunneling traffic originating at a large cloud provider via their own infrastructure to the IXP.

In future work, we plan to further assess the underlying operational practices that lead to such situations. In this work, we accept such traffic as valid, since we strive to provide an analysis of intentionally spoofed traffic.

After handling all of the above cases, and adding the corresponding IP address ranges to the valid address space of the respective IXP members, we reduce the traffic in Invalid by 59.9% of bytes resp. 40% of packets.

4.5 Cross-Check with Active Measurements

Since 2005, the CAIDA Spoofer Project [14] collects active measurement data about the "spoofability" within ASes in a crowd-sourced fashion. In a nutshell, a Spoofer software probe crafts packets with source IP addresses from various ranges and sends them to a measurement server. If the measurement server successfully receives some or all of the intentionally spoofed packets, then spoofing is possible in the AS hosting the probe. These measurements have recently been made publicly available, allowing us to cross-check active inferences of spoofability with our findings.

We leverage the available Spoofer dataset [14], containing results from measurements executed within the last year. In total, we find relevant data for 97 overlapping ASes (i.e., 8% of all IXP members under consideration).[5] Of those 97 ASes, we detected spoofed traffic (Invalid or Unrouted) for 74%. Spoofer detected spoofability in 30% of the 97 networks. Intersecting our positive detections, we find that Spoofer data agrees with our observations for some 28% of the networks for which we see spoofed traffic. Our passive approach, on the other hand, detects spoofed traffic from 69% of the networks that were tagged as spoofable by Spoofer measurements.

The quantitative differences in our measurements reflect both our different vantage points and the essential difference between the ability to spoof and actual spoofing, as carried out and visible in passive traces. Recall that for a Spoofer probe to reach the target, it has to cross multiple AS boundaries, and is thus subject to filtering, potentially by several ASes on the path. Thus, active measurements provide a lower bound on spoofability in certain networks. Contrarily, Spoofer identified several ASes as spoofable, for which we do not see any spoofed traffic. Reasons here include that there are either no hosts in these networks that do actively perform spoofing, that our inference methodology is too conservative to capture those cases, or recent changes in filtering practices (recall that we compare 4 weeks of passive measurements against one year of crowdsourced data).

Summary: This concludes our evaluation of the three different approaches to detect spoofed traffic. We chose the most conservative estimation of valid IP address space per AS, the Full Cone. During development of this approach, we encountered various limitations that go along with BGP datasets. As such, in order to get a more fine-grained estimation of the valid IP space per AS, further study of the spatial and temporal characteristics of public BGP data is needed. Our findings also highlight that leveraging external datasets to account for additional AS relationships (e.g., multi-AS organizations) is crucial in order to minimize false positive detections. We acknowledge that our resulting Full Cone considers as many as 5K ASes as legitimate sources for all of the Internet's 11M routed /24 prefixes, which likely results in significant portions of spoofed traffic that remain undetected by our approach. However, our conservative approach results in a very distilled traffic dataset

[5] We only consider ASes in which the Spoofer project conducted direct measurements, i.e., the probes were not located behind a NAT.

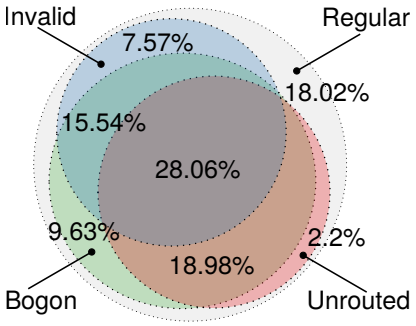


Figure 5: Percentage of members contributing traffic to the three classes: Bogon, Invalid, and Unrouted.

that is indeed mostly composed of actual spoofed traffic. Recall that the choice between the three approaches does not affect Bogon and Unrouted. We conduct all further analyses in the remainder of this paper based on the results this approach yields.

5 NETWORK PERSPECTIVE

In this section, we study which networks send what kind of illegitimate traffic. We first study filtering consistency for individual networks. Then, we take the business types of individual networks into account and contrast them with their individual traffic contribution. Finally, we identify (and remove for later analysis) some members that contribute illegitimate traffic that is not the result of intentional spoofing, but stray traffic originated from routers.

5.1 Filtering and Traffic Contribution

Filtering Consistency: The Venn diagram in Figure 5 shows what percentage of members at this IXP contribute traffic to our three classes, as well as intersections in contribution to different classes. We next use this to deduce lower bounds on which filtering strategy individual members apply. If we do not observe a member emitting flows falling in one of our categories, we assume this member filters the respective type of traffic. We are aware that this is a soft criterion, e.g., an AS may simply not emit flows with spoofed source IP addresses traversing its network during our study period. However, we argue that it is still a reasonable approximation to provide tight lower bounds, given the length of the observation period (4 weeks).

In total, we find that only some 18% of members are "clean" in the sense that they do not send any traffic classified as either Bogon, Unrouted, or Invalid. On the other end of the spectrum, we find around 28% of members contributing traffic to all of our classes. Thus, these networks do not deploy proper filtering. Another interesting case are some 9% of networks that contribute only Bogon traffic. We presume that these networks deploy filtering against spoofing, but lack filtering for bogon ranges. Of the members contributing Unrouted traffic, the vast majority, 96%, also contribute Invalid or Bogon traffic, highlighting that packets with unrouted source addresses are a good indicator for spoofing detection on a per-network level. Only some 7% of the members contribute only Invalid traffic exclusively, but do not fall in either of the other classes. Here, we can presume that they have best effort filters deployed in the sense that they use appropriate semi-static filters. Still the fact that we see traffic in Invalid suggests that they do not follow BCP38 and BCP84.

Business Types: To understand if the business types of networks directly relate to filtering setup and contribution to illegitimate traffic, Figure 6 consists of two scatterplots that show per member the total traffic contribution (x-axis), as well as the share of Bogon respectively Invalid of their individual traffic (y-axis). Note that the general observations for Unrouted are similar and since only less than 3% of members contribute Unrouted traffic exclusively, we show only the contributions for Bogon and Unrouted.

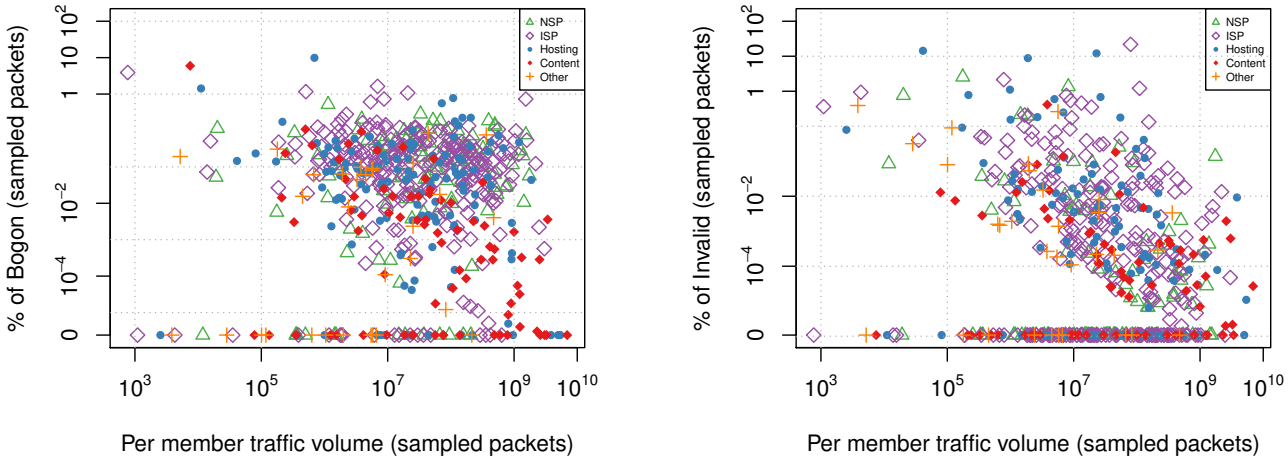
We use different plotting symbols to highlight the different business type of the member ASes, which we derive from PeeringDB [3].[6] Intuitively, members contributing more overall traffic, but a tiny share of Bogon or Invalid are located in the bottom right corner, while members with large fractions of Bogon/ Invalid traffic, but low overall traffic volume are in the upper left corner. Generally, we find that most networks with significant overall traffic shares show a comparably low fraction of illegitimate traffic, according to our classes. Indeed, most large content providers do not contribute any traffic to Bogon and only few to Unrouted. This is reasonable, since most content providers have full control over their network and almost no end-user machines.

In terms of members that have significant shares (> 1%) of Bogon, Unrouted, and Invalid traffic, we predominantly find hosting companies (highlighted with blue dots), end-user ISPs and, to a lesser extent, transit providers. These network types have in common that they typically provide connectivity (and possibly hardware), but have little control over how the provided resources are *used* by individuals (e.g., virtual machines within a hoster). In the absence of proper filtering, spoofing is more likely to be carried out from hosts within such networks, compared to e.g., large content providers. ISPs provide service for end users, which may indeed have incentives to originate spoofed traffic and they also may as well suffer from misconfigurations, which can lead to leaked traffic, e.g., from CPE NAT devices.

5.2 Spoofing vs. Stray

So far, we focused on the contribution of illegitimate traffic from individual networks, as well as their filtering strategies. We want to recall, however, that not all illegitimate traffic is in fact the result of spoofing, but can also be the result of uncommon routing policies or misconfigurations (i.e., stray traffic, recall Section 3). While we are not able to comprehensively identify and remove stray traffic from our analysis (e.g., Bogon traffic as result of misconfiguration), we found a prominent case of stray traffic that contributes to Invalid: Traffic from router IP addresses. Recall that routers have multiple interfaces each with its own IP address. A router that sends out a packet (i.e., an ICMP packet) chooses one of these IPs, often arbitrarily [7]. Since the prefixes and corresponding IP addresses for transit links between ASes are not necessarily routed at all or captured by our cone methodology, such packets contribute to Invalid. Using the CAIDA Ark traceroute dataset[13], we extracted router IP addresses from some 500M available traceroutes conducted in

[6] We classified ASes without PeeringDB entries manually.



(a) IXP members by network type: Bogon

(b) IXP members by network type: Invalid

Figure 6: Network-wide view of Spoofing: Business Types and Traffic / Filtering.

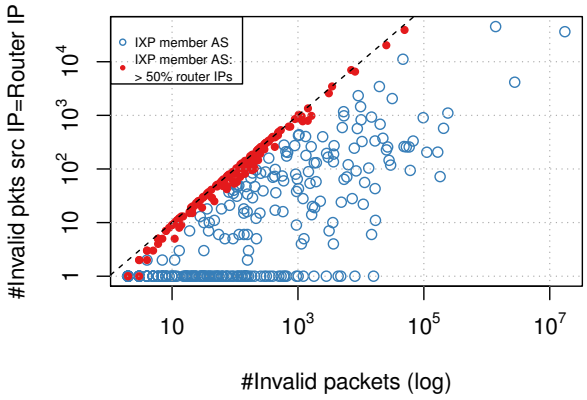


Figure 7: Router IP addresses among invalid packets per member.

February 2017, and tag the corresponding traffic originated from router IP addresses in Invalid.

The scatterplot in Figure 7 shows for each member Invalid packets vs. the number of packets with a router source IP address. We find that many members are on, or close to, the diagonal, indicating that most of their Invalid traffic comes from router IPs. While the overall contribution of router IP addresses to our Invalid class is small (less than 1%), we find it highly unlikely that a member whose Invalid packets are dominated by router IP addresses is otherwise a heavy carrier for spoofed traffic. We hence omit members whose Invalid packets consist of 50% or more packets with router IP addresses from our following analysis. This reduces the percentage of members contributing Invalid traffic from 57.68% to 39.59% . Note that this significantly reduces the number of considered members, but not the amount of Invalid traffic.

When looking at the transport layer protocol breakdown of traffic from router IP addresses, we find that about 83% of the packets are ICMP, while UDP and TCP make up for only 14.4% resp. 2.3%. The high percentage of ICMP suggests that a large fraction of this traffic is indeed stray traffic (e.g., *ping* replies from routers). We point out, however, that not all traffic from router IP addresses is necessarily stray traffic: Analysis of the UDP flows shows that 76.3% are destined towards NTP servers with only a small number of source IP addresses, which could indicate attempted reflection attacks on these particular routers (we study amplification attacks in Section 7). We acknowledge that we might discard some spoofed traffic by not considering members whose Invalid traffic consists primarily of packets with router source IP addresses.

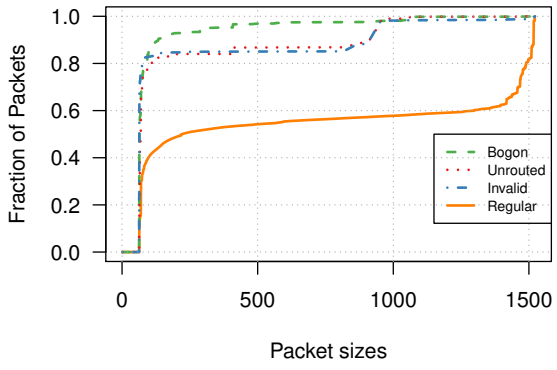
6 TRAFFIC PERSPECTIVE

In this section, we study quantitative and qualitative characteristics of Bogon, Unrouted, and Invalid traffic. To put our findings into perspective, we contrast characteristics of spoofed traffic with regular traffic exchanged at our IXP.

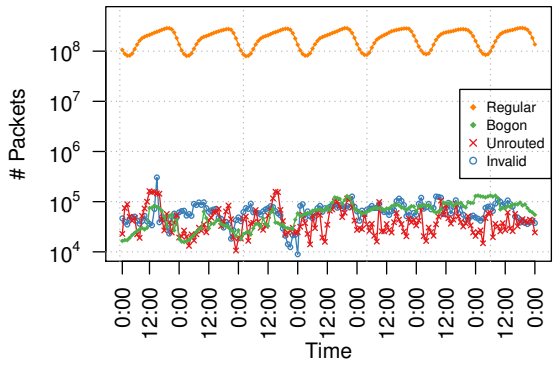
6.1 Timeseries and Packet Sizes

Figure 8a shows a CDF of packet size distributions for the different traffic classes. While regular traffic shows a typical bimodal distribution, i.e., large data-carrying packets and small ACK packets [49], spoofed traffic consists almost exclusively of small packets. In fact, more than 80% of packets in all three classes have a size less than 60 bytes. In the case of TCP, this indicates that these packets do not carry actual data, but are mere connection attempts. This strongly suggests that spoofing is less often used for volume-based attacks, but rather for SYN flooding and amplification attacks, whose return traffic (if any) is regular traffic.

With regards to time-of-day patterns (Figure 8b), our three classes of traffic again vastly deviate from regular traffic. While regular traffic shows a typical day pattern, Unrouted and Invalid traffic show a very unsteady pattern, including significant spikes. This is a first indication that this traffic is mainly caused by attacks, and not part of regular user interaction. Bogon traffic, on the other hand, shows similar irregularities, but a slight time-of-day pattern (pronounced, especially during the first three days). This suggests that Bogon does not exclusively consist of attack traffic, but also



(a) CDF: packet sizes.



(b) Time series week of 2017-02-20 (sampled pkts).

Figure 8: Traffic characteristics.

contains some stray traffic, i.e, that is likely related to unsuccessful TCP connection attempts from devices in misconfigured NAT environments, triggered by regular user behavior.

Figure 9 shows a port-based application classification of packets of our three classes, contrasted with regular traffic exchanged at the IXP. Here, we partition our port-based classification according to *(i)* direction, i.e., SRC and DST port numbers, and *(ii)* the respective transport protocol, i.e., TCP vs. UDP. We only show the six most popular port numbers, and aggregate the remaining port numbers into "other". We note that port numbers in "other" are mostly randomly distributed, suggesting ephemeral port numbers.

In the case of regular HTTP(S) traffic, we expect to see *both directions*: traffic from clients to servers, as well as traffic from servers to clients. Hence, packets from clients to servers carry 80/443 in their DST field, and reply packets from servers to clients carry 80/443 in their SRC field, and an ephemeral port number in the DST field. This interaction is well-reflected when comparing TCP DST and TCP SRC statistics for regular traffic. In the case of spoofed traffic, however, the situation is different: Here, we expect to see only *one direction*, i.e., the spoofed packet to its respective destination. Replies from the server (if any) will not fall into our spoofing categories, since they naturally carry a valid SRC IP address, the servers' address. This observation is well-reflected in our port statistics for spoofed traffic: The majority of Bogon, Invalid, and Unrouted packets carry HTTP(S) as DST address, hinting towards flooding attacks destined to HTTP(S) servers. Indeed, we find a corresponding attack pattern, which we study in Section 7.

The case of UDP traffic is even more intriguing: In the regular case, we mostly find randomly distributed SRC and DST port numbers.[7] Stunningly, we see that the DST port numbers in the case of Invalid traffic are far from randomly distributed: More than 90% of all Invalid UDP packets carry port number 123 as DST and are, hence, destined to NTP servers. Recall that NTP is prone to amplification attacks. We study the related attack patterns in detail in Section 7. Interestingly, we also notice that while Unrouted UDP traffic carries mostly random DST port numbers, port 27015 (Steam, online gaming) stands out. A recent study [17] identified this port as commonly attacked.

6.2 Address Structure

We next study spatial characteristics of the source and destination IP addresses. Figure 10 shows the distribution of packets for each class across the IPv4 address space. Here, we partition the address space in 256 /8 bins and show, for each /8, the number of sampled packets. We observe pronounced differences between our three classes of traffic.

For Unrouted packets, we find that their source addresses are mostly randomly distributed across the entire address space. The higher density of source addresses in some ranges (e.g., from 1/8 to 50/8 and 128/8 - 160/8) is caused by the fact that those address ranges simply have larger amounts of unrouted addresses than others [44]. Address uniformity is a common assumption for spoofed traffic [39]. However, we note that this is not always the case, since we observe one pronounced spike at around 200/8. Destination addresses of Unrouted packets, however, show strong concentrations on particular address blocks (and, in fact, single addresses, as we show in Section 7).

For Bogon packets, we see that the source ranges are inherently concentrated on a small subset of the address space (after all, there are only few bogon ranges). The majority falls in private address ranges (with spikes at 10/8 and 192/8). Additionally, we see multicast and, to a lesser extent, "Future Use" (right end). Hence, source addresses are not uniformly distributed across bogon ranges. This suggests that Bogon contains both shares of traffic from likely misconfigured devices (strong concentration in RFC1918 ranges), as well as traffic related to randomly spoofed source addresses (rather uniform distribution in multicast/future use ranges). Indeed, we find that the spikes in destination addresses at 192/8 and 80/8 mostly receive traffic from random IP addresses in the multicast/future use space, suggesting attacks with random Bogon source addresses.

Invalid source addresses differ significantly from the other classes. The distribution shows several peaks, indicating that some specific source addresses are spoofed much more often than others. This is a typical signature of amplification attacks and underlines that address uniformity can not be unanimously accepted as a criterion to identify spoofed traffic [48]. We find large peaks at 183/8 and 61/8. In one of the cases most of the traffic share is due to spoofed addresses routed by a large hosting company which is known to be often targeted by DDoS attacks. Closer inspection of this traffic

[7] BitTorrent is the dominant UDP-based protocol seen at this vantage point and primarily uses random port numbers [45].

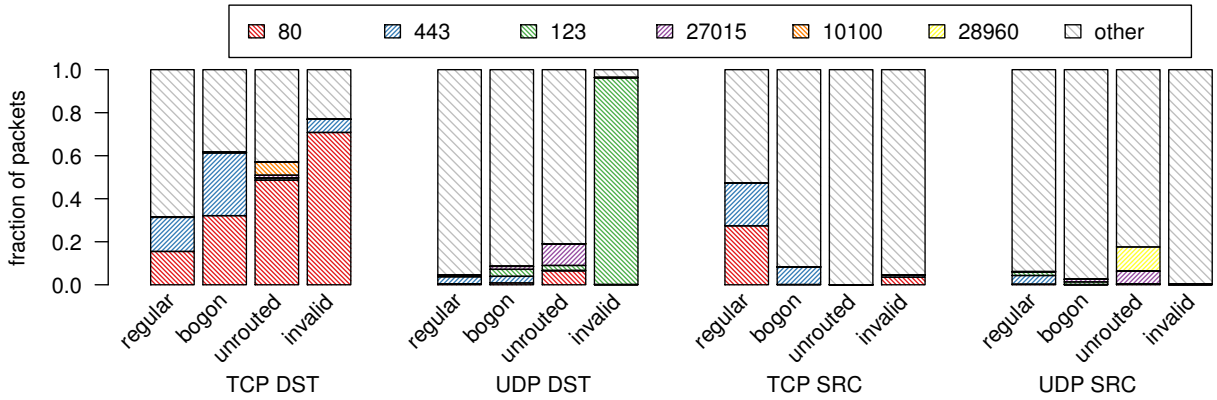
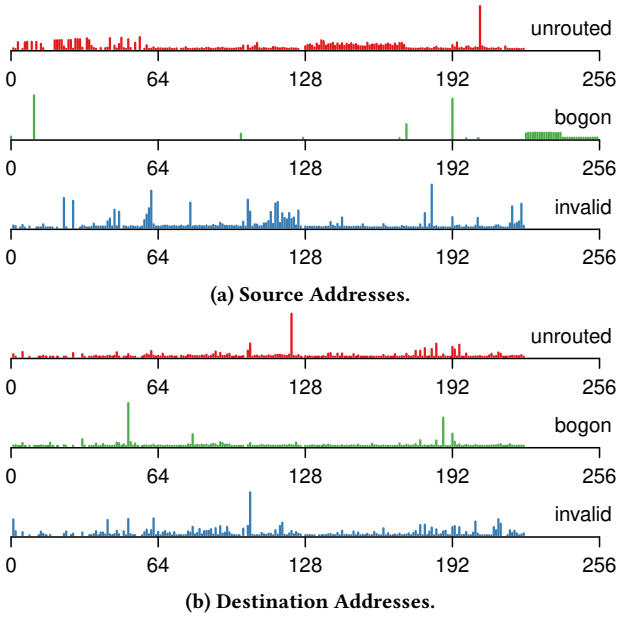


Figure 9: Traffic mix for regular, Bogon, Unrouted and Invalid traffic.



(a) Source Addresses.

(b) Destination Addresses.

Figure 10: Traffic distribution across address space.

shows that it is indeed destined to NTP servers, suggesting amplification attacks. Destination addresses again show large peaks on particular destinations. Here, we expect to see both victims of spoofing with random addresses (potentially in Invalid), as well as targeted amplifiers, e.g., NTP servers. For a detailed analysis see Section 7.

Summary: Our observations regarding traffic packet sizes, time-of-day-effects, application mix and address structure highlight large differences between regular and spoofed traffic. The characteristics we observe are well in line with different attack patterns carried out with spoofed source addresses. This indicates that our approach is effective in isolating spoofed traffic.

7 ATTACK PATTERNS

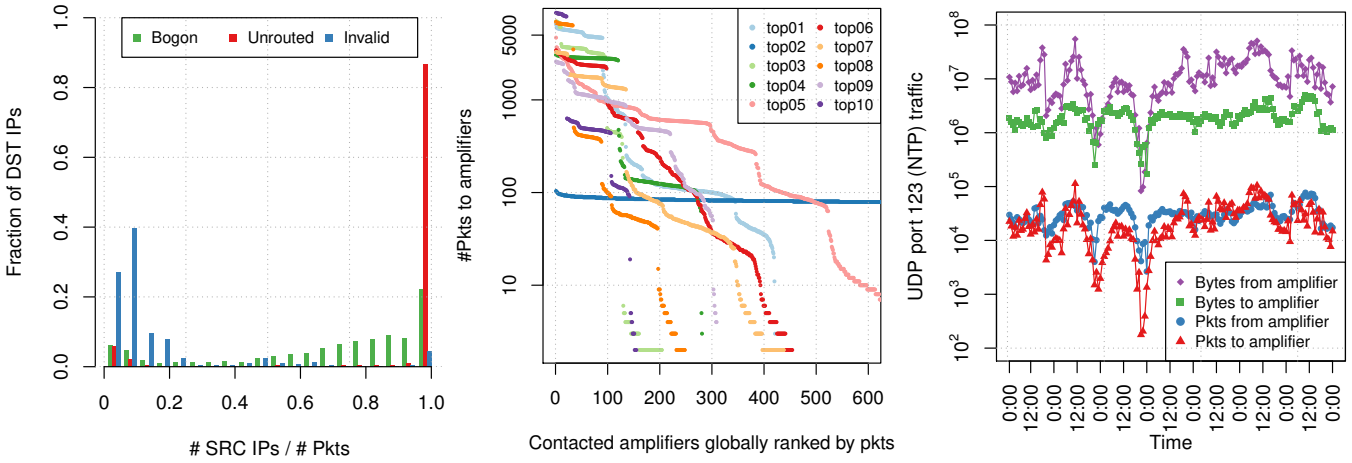
The dominant characteristics of traffic with spoofed source addresses suggest the presence of different attacks. We now take a closer look at two common attack patterns, namely amplification and flooding (recall Section 2). Recall that flooding attacks are often carried out using a wide range of source IP addresses (random spoofing), while amplification attacks require selective spoofing of source IP addresses of victims.

Selective vs. Random Spoofing: To study selective vs. random spoofing events, we first isolate the set of destination IP addresses for which we sampled more than 50 Unrouted, Bogon, or Invalid packets (8.4K, 19.7K and 9.7K, respectively).[8] Then, we calculate for each destination the ratio of source IP addresses vs. received packets. Figure 11a shows a breakdown of this ratio for the destinations, partitioned by the class of traffic. Destinations falling in the leftmost bin received traffic only from very few (or one single) IP addresses. Consequently, IP addresses in the rightmost bin received every single packet from a different source address.

Here, we observe a striking difference when comparing the three classes: Close to 90% of destinations of Unrouted traffic receive every single packet from a unique source IP address. This highlights that the vast majority of packets with Unrouted source addresses are due to random spoofing attacking a single destination. In fact, the top 5 destinations receive an upward of 2.3 billion packets over the course of four weeks (sampling extrapolated) from random source addresses. Interestingly, we also see that a significant share of destinations in Bogon addresses show high degrees of source address uniformity, yet with a lesser extent and with some 2.51% that receive significant traffic only from one single IP address. Invalid is the most intriguing case: Here, we see that some comparably small fraction of destination IP addresses receive uniformly spoofed addresses (rightmost bin), but the majority of target addresses receive Invalid traffic from a small set of source addresses (see spikes in the left area of the plot). This is the signature of amplification attacks, where attackers specifically craft packets with spoofed source addresses of their victims, and send packets towards amplifiers.

NTP Amplification: Recall that Invalid traffic is typically *selectively* spoofed and that the vast majority of Invalid UDP packets

[8] Note, 50 sampled packets extrapolate to some 500K packets exchanged via the IXP.



(a) Ratio of #spoofed SRC IPs vs. #packets to DST (DSTs with > 50 sampled pkts).

(b) Ranked NTP amplifiers (x-axis) and corresp. pkts (y-axis) for top10 victims.

(c) Time series: NTP attack (INVALID) and response (regular) for week 3.

Figure 11: Attack patterns: Selectively vs. uniformly spoofed source IPs.

is directed to NTP servers. We also found that a single member at the IXP is responsible for 91.94% of all INVALID NTP traffic and the top 5 members together emit more than 97.86% of INVALID NTP. During our observation period, we see NTP trigger traffic from 7,925 individual IP addresses sent by 44 members towards 24,328 possible amplifiers. We compare the list of our 24,328 destinations against a list of some 1.3M NTP servers derived from ZMap scans [4] executed February and March 2017 and find an overlap of 3,865 addresses. Comparing with ZMap scans from December 2016 and January 2017 we find less than 1.8K and 2K hits.

To gain a better understanding of the underlying strategy of some of the largest amplification attacks, we plot in Figure 11b for the top 10 victims (i.e., source addresses of trigger traffic) the number of amplifiers ranked by packets (x-axis) and the number of trigger packets sent to each amplifier (y-axis). Here, we observe different attack patterns: Some amplification attacks involve only a handful of amplifiers (90) receiving the bulk of trigger traffic. Other strategies involve using a large number of amplifiers and distributing trigger traffic uniformly across them (as in the case of top-2, 13,377 amplifiers contacted). To assess the effect of amplification, we isolate those IP pairs, for which we are able to see both the trigger traffic to the amplifier, as well as the amplifiers' response packets to the victim. Figure 11c shows a timeseries of packets and bytes sent towards amplifiers (trigger traffic), as well as the responses. Here, we see that amplification indeed works: While the number of packets in both directions is similar (and tightly correlated), the number of bytes returned by the amplifiers exceeds the trigger traffic by an order of magnitude. An interesting observation of how amplification attacks manifest at our vantage point.

Summary: Our analysis of attack patterns allows us to illuminate both how attackers carry out flooding and amplification attacks, as well as how these attacks manifest in inter-domain traffic. We see evidence of both random spoofing attacks as well as sophisticated amplification attacks, where attackers rely on different strategies to select amplifiers. In the case of amplification attacks, our vantage point allows us to not only study attack strategies, but to also partially expose their eventual effect on victims, i.e., the resulting traffic from amplifiers.

8 CONCLUSION

In this paper, we present a new approach for passive detection of spoofed traffic. Our method enables us to detect if individual networks allow for spoofing and to isolate spoofed traffic and study its properties. We apply and evaluate our approach in practice, studying spoofed traffic exchanged between some 700 networks peering at a major European IXP. We find that the majority of connected networks do not filter consistently and allow traffic with spoofed source IP addresses to be injected into the Internet. Our analysis of the properties of spoofed traffic "in the wild" yields hard-to-get insights into both the dominant characteristics of this type of traffic as well as into detailed patterns of attacks carried out with such traffic. While we chose an IXP—due to its locality and the amount of connected networks—our method is not limited to this vantage point. In principle, every network on the inter-domain Internet can opt to apply it to filter its incoming traffic, or to detect spoofing. For now, our methodology provides a very conservative overestimation of the valid IP address space per AS. We intentionally sacrificed the specificity of a closer estimation in order to reduce misclassifications in INVALID. Future work includes better recognition of stray traffic and refining the construction of AS-specific prefix lists to achieve tighter bounds when estimating the valid IP space per network. This entails a thorough study of the size and completeness of the BGP-derived address spaces per AS, as well as improving methods to derive additional AS relationships from external data.

ACKNOWLEDGMENTS

We want to express our gratitude towards the IXP operators for their support and feedback. We thank the network operators who participated in our survey. We thank our shepherd Dan Pei and the

anonymous reviewers for their helpful feedback. This work was partially supported by Leibniz Prize project funds of DFG/German Research Foundation (FKZ FE 570/4-1).

REFERENCES

[1] Mutually Agreed Norms for Routing Security (MANRS). https://www.routingmanifesto.org/manrs/.
[2] North American Network Operators' Group. https://www.nanog.org/.
[3] PeeringDB facilitates the exchange of information related to Peering. https://peeringdb.com/.
[4] Rapid7 Labs, Project Sonar UDP Scans. https://scans.io/study/sonar.udp.
[5] RIPE Routing Working Group. https://www.ripe.net/participate/ripe/wg/routing.
[6] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker. Accountable internet protocol (aip). In *ACM SIGCOMM*, 2008.
[7] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. Avoiding traceroute anomalies with Paris traceroute. In *ACM SIGCOMM*, 2006.
[8] F. Baker and P. Savola. Ingress Filtering for Multihomed Networks. RFC 3704 (Best Current Practice), Mar 2004.
[9] P. Barford, R. Nowak, R. Willett, and V. Yegneswaran. Toward a model for source addresses of internet background radiation. In *PAM*, 2006.
[10] R. Beverly and S. Bauer. The Spoofer project: Inferring the extent of source address filtering on the Internet. In *USENIX SRUTI*, 2005.
[11] R. Beverly, A. Berger, Y. Hyun, and kc claffy. Understanding the Efficacy of Deployed Internet Source Address Validation Filtering. In *ACM IMC*, 2009.
[12] X. Cai, J. Heidemann, B. Krishnamurthy, and W. Willinger. Towards an AS-to-Organization Map. In *ACM IMC*, 2010.
[13] CAIDA. Ark Measurement Infrastructure. http://www.caida.org/projects/ark/.
[14] CAIDA. Spoofer Project. https://www.caida.org/projects/spoofer/.
[15] Z. Chen, C. Ji, and P. Barford. Spatial-temporal characteristics of internet malicious sources. In *IEEE INFOCOM*, 2008.
[16] M. S. Cotton and L. Vegoda. Special Use IPv4 Addresses. RFC 5735, Oct 2015.
[17] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *ACM IMC*, 2014.
[18] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *ACM IMC*, 2014.
[19] A. Dainotti, K. Benson, A. King, kc claffy, E. Glatz, and X. Dimitropoulos. Estimating Internet Address Space Usage Through Passive Measurements. *ACM SIGCOMM CCR*, 44(1), 2014.
[20] A. Dainotti, K. Benson, A. King, kc claffy, E. Glatz, X. Dimitropoulos, P. Richter, A. Finamore, and A. Snoeren. Lost in Space: Improving Inference of IPv4 Address Space Utilization. Tech. rep., CAIDA, Oct 2014. http://www.caida.org/publications/papers/2014/lost_in_space/.
[21] J. Durand, I. Pepelnjak, and G. Doering. BGP Operations and Security. RFC 7454 (Best Current Practice), Feb 2015.
[22] W. Eddy. TCP SYN Flooding Attacks and Common Mitigations. RFC 4987 (Informational), Aug 2007.
[23] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice 38), May 2000. Updated by RFC 3704.
[24] Y. Gilad and A. Herzberg. LOT: a defense against IP spoofing and flooding attacks. *ACM Trans. Computer Systems*, 15(2):6, 2012.
[25] V. Giotsas and S. Zhou. Improving the discovery of IXP peering links through passive BGP measurements. In *IEEE INFOCOM*. IEEE, 2013.
[26] B. Huffaker, K. Keys, R. Koga, and M. Luckie. Caida inferred as to organization mapping dataset.
[27] A. Hussain, J. Heidemann, and C. Papadopoulos. A Framework for Classifying Denial of Service Attacks. In *ACM SIGCOMM*, 2003.
[28] M. Kührer, T. Hupperich, J. Bushart, C. Rossow, and T. Holz. Going wild: Large-scale classification of open DNS resolvers. In *ACM IMC*, 2015.
[29] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *USENIX Security*, 2014.
[30] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks. In *WOOT*, 2014.
[31] B. Liu, J. Bi, and A. V. Vasilakos. Toward incentivizing anti-spoofing deployment. *IEEE Transactions on Information Forensics and Security (TIFS)*, 9(3):436–450, 2014.
[32] B. Liu, J. Bi, and Y. Zhu. A deployable approach for inter-AS anti-spoofing. In *IEEE ICNP*, 2011.
[33] X. Liu, A. Li, X. Yang, and D. Wetherall. Passport: Secure and Adoptable Source Authentication. In *NSDI*, 2008.
[34] Q. Lone, M. Luckie, M. Korczyński, and M. van Eeten. Using loops observed in traceroute to infer the ability to spoof. In *PAM*, 2017.
[35] M. Luckie, B. Huffaker, kc claffy, A. Dhamdhere, and V. Giotsas. AS Relationships, Customer Cones, and Validation. In *ACM IMC*, 2013.
[36] M. Luckie, K. Keys, R. Koga, B. Huffaker, R. Beverly, and kc claffy. Software systems for surveying spoofing susceptibility, 2016.
[37] R. Miao, R. Potharaju, M. Yu, and N. Jain. The Dark Menace: Characterizing Network-based Attacks in the Cloud. In *ACM IMC*. ACM, 2015.
[38] J. Mirkovic and E. Kissel. Comparative Evaluation of Spoofing Defenses. *IEEE Trans. Dependable Secur. Comput.*, 8(2):218–232, Mar 2011.
[39] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage. Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)*, 24(2):115–139, 2006.
[40] R. T. Morris. A Weakness in the 4.2BSD Unix TCP/IP Software, 1985.
[41] G. Moura, R. de O. Schmidt, J. Heidemann, W. B. de Vries, M. Muller, L. Wei, and C. Hesselman. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. In *ACM IMC*, 2016.
[42] C. Perkins. IP Mobility Support for IPv4. RFC 3344 (Proposed Standard), Aug 2002. Obsoleted by RFC 5944, updated by RFCs 4636, 4721.
[43] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address Allocation for Private Internets. RFC 1918 (Best Current Practice), Feb 1996. Updated by RFC 6761.
[44] P. Richter, M. Allman, R. Bush, and V. Paxson. A Primer on IPv4 Scarcity. *ACM Computer Communication Review*, 45(2), 2015.
[45] P. Richter, N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger. Distilling the Internet's Application Mix from Packet-Sampled Traffic. In *PAM*, 2015.
[46] P. Richter, G. Smaragdakis, A. Feldmann, N. Chatzis, J. Boettger, and W. Willinger. Peering at Peerings: On the Role of IXP Route Servers. In *ACM IMC*, 2014.
[47] RIPE NCC. RIPE Routing Information Service (RIS). https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris.
[48] C. Rossow. Amplification hell: Revisiting network protocols for DDoS abuse. In *NDSS*, 2014.
[49] R. Sinha, C. Papadopoulos, and J. Heidemann. Internet Packet Size Distributions: Some Observations. Technical Report ISI-TR-2007-643, USC/Information Sciences Institute, May 2007. Orignally released October 2005 as web page http://netweb.usc.edu/%7ersinha/pkt-sizes/.
[50] F. Soldo, A. Markopoulou, and K. Argyraki. Optimal Filtering of Source Address Prefixes: Models and Algorithms. In *IEEE INFOCOM*, 2009.
[51] Team Cymru. THE BOGON REFERENCE. http://www.team-cymru.org/bogon-reference.html.
[52] University of Oregon. Route Views Project. http://bgplay.routeviews.org.
[53] J. Weil, V. Kuarsingh, C. Donley, C. Liljenstolpe, and M. Azinger. IANA-Reserved IPv4 Prefix for Shared Address Space. RFC 6598 (Best Current Practice), Apr 2012.
[54] J. Wu, G. Ren, and X. Li. Source Address Validation: Architecture and Protocol Design. In *IEEE ICNP*, 2007.
[55] G. Yao, J. Bi, and A. V. Vasilakos. Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter. *Transactions on Information Forensics and Security*, 10(3):471–484, March 2015.
[56] G. Yao, J. Bi, and P. Xiao. Source address validation solution with OpenFlow/NOX architecture. In *IEEE ICNP*, 2011.
[57] L. Zhu, Z. Hu, J. Heidemann, D. Wessels, A. Mankin, and N. Somaiya. Connection-Oriented DNS to Improve Privacy and Security. In *IEEE SP*, 2015.