2025 36th International Teletraffic Congress (ITC 36)

DDoS on Repeat: Measuring Pulse-Wave DDoS in the Wild

Daniel Kopp
DE-CIX & University of Kassel

Oliver Hohlfeld
University of Kassel

***Abstract*—This paper investigates the recent phenomenon of pulse-wave DDoS attacks and studies the characteristics and prevalence of pulsed DDoS attacks in the wild. Despite historical and recent references, no study quantified these attacks on the Internet. The scarcity of measurement studies could be attributed to uncertainty and the inherent challenge of identifying pulsed DDoS attacks, or lack of awareness of the extent of these attacks. Leveraging a dataset captured at a major IXP over four months, we identify pulse-wave attacks from sampled flow-traces, providing insight into 10,000 DDoS attacks. Surprisingly, we observe that 27% of all observed DDoS attacks can be attributed to pulse-wave DDoS events. This shows that pulsed DDoS attacks have emerged as a significant attack tactic and should be considered in future work.**

***Index Terms*—Internet measurements, DDoS, IXP**

I. Introduction

One of the most prevalent cybersecurity threats to date is the execution of Distributed Denial-of-Service (DDoS) attacks [1], [2], [3], [4]. These attacks target applications or service providers by exceeding the available critical resources, such as computing resources or network bandwidth. The motivations driving these criminal activities are diverse and encompass factors such as financial gain [5], [6], political motivations [7], [8], and instances of cyber warfare [9], [10].

DDoS attacks are frequent (e.g., thousands of attacks can be observed at an IXP every single day [11]), they can be conducted without technical expertise [12], and can generate significant attack volumes, reaching up to 3.5 Tbit/s as observed in late 2021 [13]. Such high volumes can even threaten the largest networks [13], [14], [2], [15]. The properties of traditional DDoS attack types are well understood (see, e.g., [16], [11], [17]), and mitigation solutions such as traffic scrubbing [18], [19], [20], [21], [22], [17] or traffic blackholing [23], [20], [24], [25] exist. Yet, the emergence of new attack vectors challenges DDoS mitigation and thus provides harm to the Internet at large.

In this context, a relatively unexplored method of attack is the tactic of sending repeated DDoS pulses, so-called *pulse-wave* or *pulsed attacks*. A pulse-wave DDoS attack is characterized by short, intense bursts of traffic sent at regular intervals to overwhelm a target's network or service, to evade traditional mitigation systems [26]. While the attack vector of pulse-wave attacks has been recognized for some time [27], [28], [29], [30], [31], and initial mitigation approaches based on artificial traffic have been proposed [26], comprehensive studies quantifying these attacks in real-world settings are lacking. One potential reason can be the fact that—as we will show—they are substantially more challenging to infer than classical, continuous DDoS attacks. Moreover, The question of the extent to which pulsed DDoS attacks occur in practice is still unanswered. Figure 1 shows a pulse-wave attack pattern observed at an IXP, which, as we will show, can often be observed.

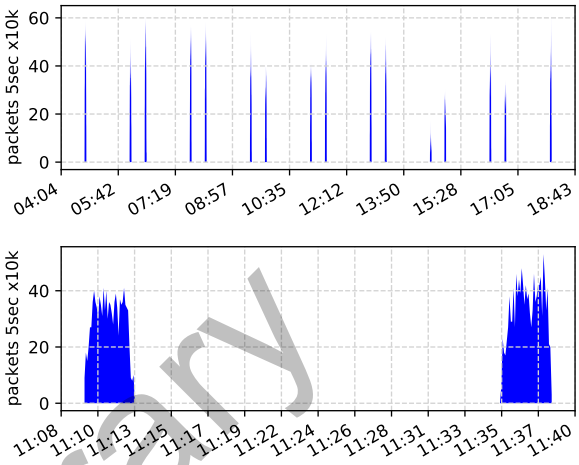


Fig. 1: A pulse-wave DDoS attack observed at an IXP: Overview (left) and detailed view (right).

Pulse-wave attacks feature several waves of attack traffic that target a victim at intervals, as opposed to a continuous stream of traffic as in traditional continuous DDoS attacks. While continuous DDoS attacks have been extensively studied, pulsed attacks are still underexplored, and their distinctive properties are poorly understood. Typical studies aim at identifying individual attacks (e.g., [11]), but when pulsed attacks are not accounted for, the reported number of attacks tends to be inflated. This and similar patterns of DDoS attacks can be frequently observed from DDoS mitigation infrastructures (e.g., IXP blackholing). However, the mere observation of this traffic pattern suggests that such patterns stem from the dynamics of Internet routing and distortion of traffic measurements. We thus aim to close this gap.

978-3-948377-03-8/19/$31.00

In this paper, we show the existence of *pulsed DDoS attacks* in Internet traffic captured at a major IXP. Within four months, we observed 102 pulsed DDoS events—their individual 2,870 attack pulses comprise 27% of all observed DDoS events. These attacks largely use standard amplification protocols (e.g., DNS for more than 80% of the attack traffic), similar to classical DDoS attacks [11].

To identify pulse-wave attacks, we present an approach that can infer pulsed attacks from sampled flow-level traces and rule out potential biases from Internet measurement artifacts. Our goal is not to identify all possible pulse-wave attacks but rather to adopt a conservative approach to inferring those that are surely pulse-wave.

With this, we characterize for the first time pulse-wave attacks in Internet traffic and demonstrate that they occur more often than previously believed. The prevalence of pulsed attacks in many attack campaigns has direct implications for Internet measurement studies. Studies that count pulses as separate DDoS incidents, without considering attack campaigns involving pulsed attacks, will inevitably overestimate the number of attack campaigns. We intend to raise awareness on the extent of pulsed DDoS attacks, which is valuable to provide more efficient DDoS mitigation processes. This way, we aim to pave the way for the broad study of pulsed DDoS attacks in the future. Our main contributions are as follows:

- **Challenges in detecting pulsed DDoS attacks:** We show that identifying pulsed DDoS attacks in Internet traffic is a challenging measurement problem (§ IV).
- **Detecting pulsed DDoS from flow-traces**: We propose an approach (§ V) to identify pulsed attacks from sampled flow-level traces at IXPs. Our approach incorporates components that emerged from discussions with industry experts and accounts for confounding factors such as route flapping.
- **Characterization of pulsed DDoS attacks**: We use this approach to characterize and quantify pulsed DDoS attacks in the wild (§ VI). We observe standard amplification protocols to be used within attacks.
- **Extent of the pulsed DDoS attack landscape**: We base our study on four months of attack traffic data captured at a major IXP. Our results show that pulsed DDoS attacks exist at a notable share, which stands in stark contrast to the general awareness of this type of DDoS attack.

II. Background and Related Work

DDoS Attacks, Amplification Protocols and Mitigation: The main reason for the scale of current DDoS attacks [32], [33], [34], [35] is the abuse of specific protocols to amplify attack traffic [1], [2], [3]. To enable DDoS, responses to spoofed traffic [36], [37], [38], [39], [40], i.e., packets with modified source IP addresses, are reflected toward the DDoS target and not the original sender. The reflected traffic is not only sent to a different target, but also *amplified*, since a small request can trigger significantly larger responses (up to $\times 50,000$) [41], [16], [42]. The so-called amplification factor depends on the abused protocol, e.g., NTP, DNS, or more recently Memcached [16], [43], [44], [11]. To mitigate these attacks in practice, various reactive DDoS mitigation techniques filter unwanted attack traffic, e.g., scrubbing services [18], [19], [20], [21], [22], [17], [45], blackholing [23], [20], [24], [25], flow samples [46], or ACLs and Flowspec [47], [48]. In this arms race, spontaneously appearing new amplification vectors are quickly growing to cause substantial harm even to well-positioned networks and applications [44], [2]. To make matters worse, once exploited protocols for DDoS often remain a threat for decades, despite the joint effort of the research community, operators, and policymakers.

Pulse-Wave DDoS Attacks: A new type of attack emerged to bypass current DDoS mitigation systems: pulse-wave attacks [27], [28], [29], [30], [31]. These attacks employ high-rate traffic pulses that are too short for traditional mitigation solutions to effectively counteract against the victim. In 2023, a new type of CDN-assisted pulse-wave attack type was identified [28], leveraging existing CDN infrastructure to concentrate attacks temporally. Addressing the challenge posed by high-intensity pulses, a congestion control-based mitigation scheme designed to operate within programmable switches was proposed in 2022 [26].

However, despite the extensive body of research on DDoS attacks, a comprehensive study regarding the prevalence of these attacks on the Internet remains absent.

III. IXP Vantage Point and Data Set

We partner with a major IXP providing sampled flow, blackholing, and BGP data to study pulse-wave attacks.

Blackholing Data Sets. Our data set is based on traffic that is intentionally dropped (null routed) by the receiving networks (blackholing). Blackholing is a standardized operational practice [49] enabling network operators to signal neighboring networks (routers) to drop traffic directed to the announced IP prefix. The data set comprises flows that match classical IP-based blackholing (i.e., all traffic to the IP prefix in the BGP announcement, with a blackholing community tag, is dropped) or advanced port-based blackholing. Advanced blackholing provides more fine-grained options for filtering traffic in the event of DDoS attacks, and is therefore more effective over a voluntary acceptance of classical blackholing routes by networks connected to the IXP.

We remark that blackholing contains all dropped traffic, which is not only DDoS. In § V, we describe a methodology for inferring pulsed DDoS attacks.

The captured data set spans 5 months, from 2023-05-01 to 2023-09-01 (see Table I). Within this data set, we found 46,766 unique destinations for potential DDoS attacks using classical blackholing and 33,312 for advanced blackholing. This gives a total of 80,078 potential DDoS targets. The blackholing data set is used as input data containing unwanted traffic (not only

	volume	flows	targets	ASNs	IXP ASNs
BH1	0.69 PByte	54m	46k	864	199
BH2	2.74 PByte	596m	33k	99	28

TABLE I: Data set: BH1 refers to the classical and BH2 denotes advanced blackholing.

DDoS). Our methodological contribution will be to present an approach in § V to infer pulsed DDoS attacks reliably.

Ethical Considerations: We carefully take several steps to ensure that all processed data is captured and used in accordance with ethical standards. We follow ethical practices and employ data-preserving methods; e.g., by studying pulse-wave DDoS attacks in blackholing data, where attack targets are publicly visible within the IXP-looking glasses. We immediately obfuscate sensitive data, i.e., IP addresses and MAC addresses. Capturing the data is compliant with the local legal regulations.

Limitations: We focus on amplification of DDoS and, therefore, acknowledges that some attack vectors may not be entirely visible. Furthermore, the visibility of Internet traffic is constrained by our vantage point (as with any Internet measurement). These limitations are reasonable, given that the study aims to provide a methodology for characterization of these attack types as visible in the wild.

IV. Detecting Pulse Waves is Hard

Correctly characterizing pulse-wave DDoS attacks in Internet traffic is a challenging problem, which might explain why currently no study has characterized pulse-wave attacks in the wild. So why is observing a single consecutive DDoS attack (as in many studies, e.g., [11]) comparably easy, while correctly characterizing a consecutive wave of DDoS attacks is hard? Unlike in controlled experiments or testbed studies (e.g., [26]), traffic spikes (pulses) in Internet traffic can be the result of different confounding effects, which we detail next. While their traffic that mimics pulsed attacks, they are not.

A. Influence by DDoS mitigation

A reliable source for observing DDoS attacks is monitoring mitigation services (e.g., traffic filtering, blackholing, traffic scrubbing). Examining the traffic of targets under attack within the sinkholes of DDoS mitigation mechanisms reveals pulse-wave DDoS patterns.

However, the first challenge emerges when consecutive DDoS attacks occur within the sinkholed traffic. This raises questions about whether this represents the complete traffic sequence or if the observed pattern results from the network operator (quickly) enabling and disabling mitigation in response to the DDoS attack. Therefore, the resulting traffic in the sinkhole can falsely mimic a pulsed pattern (see Figure 2).

B. External Factors and Route Changes

External factors and route changes/flapping can further distort DDoS traffic and mimic pulse-wave patterns. Route changes—induced by DDoS attack mitigation efforts or route flapping—possibly resulting from the DDoS attack itself, could transform steady DDoS traffic into a pulse-wave-like traffic pattern (see Figure 3).

When characterizing pulse-wave patterns of DDoS attack traffic from core Internet infrastructures such as IXPs, the path of DDoS traffic might shift between available alternative paths (e.g., between transit and peering). Although this scenario is possible and needs consideration, the exact influence on traffic

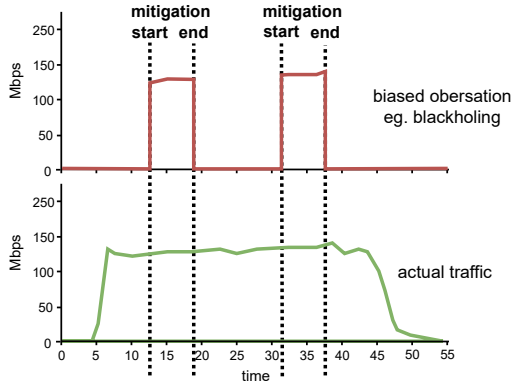


Fig. 2: DDoS mitigation may introduce bias: while the attack traffic (green, bottom plot) is continuous, quickly enabling and disabling the migration service causes traffic pulses.

patterns depends on DDoS sources, targets, and the dynamics of inter-domain routing. This could potentially lead to traffic being shifted in elongated patterns instead of shorter and more immediate changes observed within DDoS patterns. However, BGP route changes can also be related to DDoS attacks and observed traffic patterns and must be considered.

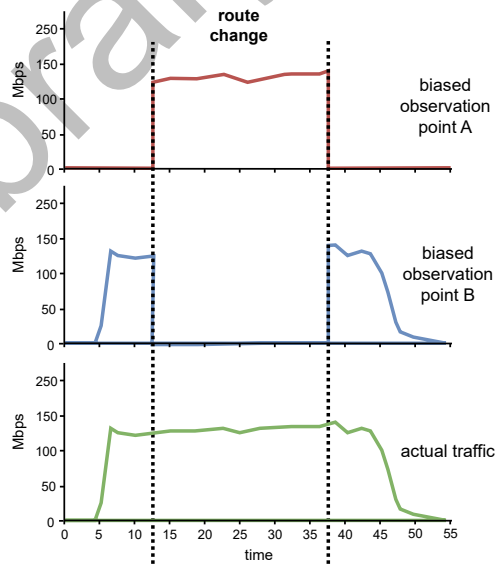


Fig. 3: Distortion of observed DDoS traffic occurs due to route changes, such as route flapping. An ideal scenario is described where traffic shifts as a whole between two observation points.

C. Influence by DDoS Detection Approach

A third major influence factor is the use of the DDoS detection approach itself. To illustrate this concept, we show the effect of a threshold within a DDoS detection approach in Figure 4. This approach can lead to various effects, artificially introducing consecutive pulse-wave patterns of DDoS attacks in the resulting dataset; *i)* In the simplest case, a DDoS attack that might be part of a pulse-wave pattern could be omitted due

to staying below the detection threshold; *ii)* More importantly, DDoS attacks not part of a pulse-wave could falsely mimic a pulse-wave pattern if their characteristics trigger the threshold occasionally. This is particularly significant when dealing with a wide variety of previously unknown traffic patterns, which are common in real-world Internet traffic data.

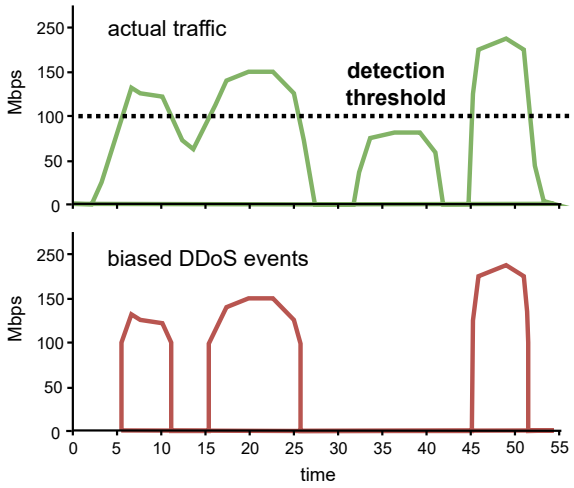


Fig. 4: Using and adjusting thresholds can lead to different sequences of DDoS events.

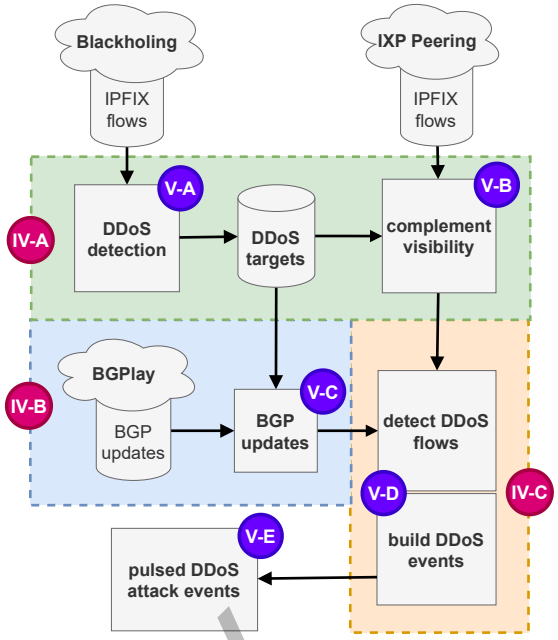


Fig. 5: Approach in characterizing pulsed DDoS attacks (section references in purple circles) and detection challenges (section references in red circles).

D. Influence by Flow Monitoring

In addition to these challenges introduced by Internet dynamics, technical challenges exist that shape the ability and limits of characterizing the details of pulse-wave-like DDoS patterns. In large Internet infrastructures, traffic monitoring and measurements are typically based on network flows (NetFlow, IPFIX) exported by network equipment. Exporting these statistical data inherits caching mechanisms that influence the timeliness and resolution of the statistics. Thus, the lowest capture resolution is driven by the concrete implementation of the flow exporter (15 seconds in our case). Awareness and tuning of all these components can limit the detection of pulse-wave DDoS attacks, and this needs to be taken into account.

All these challenges and aspects must be considered when classifying pulse-wave DDoS attacks in the wild. These challenges significantly distinguish pulse-wave DDoS from the detection and classification of individual DDoS events, potentially contributing to the scarcity of reports that describe and quantify this phenomenon in the wild.

V. How to Detect Pulse Wave DDoS

We next describe a 5-step approach (Fig. 5) to infer pulse-wave DDoS attacks from sampled, flow-level traffic traces.

A. Building a robust set of candidates

Our first step involves the identification of candidate DDoS attacks (note: not necessarily pulsed attacks) from blackholing traffic at IXPs. This is necessary since blackholed traffic can also include benign traffic. For this first filter step, we rely on previous work [11] that proposed a threshold-based approach to detect general types of DDoS attacks at IXPs. We detect label flows as DDoS attack if the sum of traffic for all flows exceeds a threshold of 100 Mbit/s, and port numbers of known amplification protocols are used. We remark that our aim is not to detect all possible DDoS attacks in our input data but rather to focus on attacks with higher confidence and thus stick to this rather conservative threshold. We manually curated a list of 50 amplification protocols that we detect, shown in Table II. This method generates a list of DDoS targets with their attack times and vectors. However, applying this step directly to IXP traffic flows could create artificial pulse-wave patterns (see § IV-C).

B. Complementing visibility on DDoS

Using blackholing datasets provides additional confidence to build a robust set of DDoS candidates. However, DDoS attacks observed through blackholing may suffer from incompleteness in two ways: 1) inadequate traffic coverage, since only a subset of peers accepts blackholing at the IXP (in traditional blackholing), and 2) time-biased DDoS traffic due to the activation and deactivation of blackholing (our first challenge described in § IV-A). To address these limitations, we enrich our data set with traffic flows from outside the blackholing by using the knowledge of the attack vectors: start time, end time, target, protocol, and source port. With that, we generate a more comprehensive representation of each DDoS attack. This step is crucial for characterizing time-based traffic patterns in

Attack Vector / Amplification Protocol	Port Numbers
mFTP	349
IKE	4500
Game	20800, 27005, 27017, 27960, 28015
SNMPv2	161, 1514
Portmap/RPC	111
Steam Protocol	27015
Web Service Dynamic Discovery	3702
Quicktime Streaming Server	7240, 8001, 8000, 7001, 9658, 9996, 8698
mFTP	6622
MacOS RPC	866
Omnilink	3904
Cinderella Collaboration	3770
Remote Replication Agent Connection	5678
Influence	3345
Folio Remote Server	2242
XeCP Node Service	3940
SQL-Net	150
ARMS	3283
BitTorrent	6881
chargen	19
CoAP	5683
DHCP Discovery	37810
D/TLS	443
IPMI	623
ISAKMP	500
L2TP	1701
mDNS	5353
Memcached	11211
MS SQL	1434
NetBIOS	137
NTP	123
OpenVPN	1194
PMSSDP	32414, 32410
QOTD	17
RDP	3389
rpcbind	873
Sentinel	1514, 5093
SIP	5060
SLP	427
SSDP	1900
tFTP	69
TP240	10074
Ubiquiti	10001, 5514, 3478
Unreal	6500, 7777, 7778, 7779, 7780
LDAP	389
SADP	37020
BACNet	47808
Kad	751
RIPv1	520
DNS	53

TABLE II: DDoS Attack Vectors and Port Numbers

DDoS attacks, eliminating noise, and addressing the challenge described in § IV-A.

C. Observing BGP route changes

To mitigate the impact of route changes, which could artificially introduce slow pulse-wave patterns (see challenge § IV-B), we leverage BGP updates over time for each potential pulse-wave DDoS attack. From the BGPlay API, we retrieve all BGP updates related to a DDoS target for the time of the attack and then correlate the sequence of BGP updates with the sequence of DDoS events to rule out any effects caused by route changes, such as route flapping, which could lead to a pulse DDoS pattern at specific vantage points. However, as noted in § IV-B, BGP updates can result from DDoS attacks themselves; nevertheless, we include the possibility of route flapping as a potential source of false positive events.

D. Finding consecutive DDoS attacks

Accurately characterizing a sequence of DDoS attacks involves observing and detecting the complete traffic pattern to be able to correctly detect the start, end, and duration of an attack. This fourth step of our approach aims to mitigate the challenge of biasing effects introduced by fixed thresholds (challenge § IV-C). Therefore, we rerun the DDoS detection from § V-A without any threshold on the full traffic flows for each DDoS target for the day of an attack. Additionally, we decrease the traffic binning to 15 seconds (see § IV-D) from the initial and typical binning of 1 minute in step 1 (§ V-A). This adjusted time binning enables the description of individual DDoS attacks, providing a balance between the limitations of flow data and the ability to characterize pulsed DDoS attacks down to a resolution of 15 seconds. From this step, we can compile a list of consecutive DDoS attacks, in which, for a target, per day, and attack vector, we describe the duration of each attack, the pause between attacks, and the traffic levels that we observe during each attack event. Based on this data set, we analyze consecutive attacks and detect pulse-wave-like DDoS events in the next step.

E. Identification of pulsed DDoS attacks

We identify pulse-like DDoS attack events from the list of consecutive DDoS attacks against specific targets, built-in § V-D. In contrast to general repetitive DDoS attacks (depicted in Figure 11 (c)), pulse-wave DDoS events employ a uniform pattern with respect to the duration of pulses and intermediate pauses. Therefore, we compile different parameters for each sequence of consecutive DDoS attacks against the same target. We use the ratio between the average duration and the median duration of the attack sequences (Figure 6). Furthermore, we employ the entropy of a sequence of durations (Figure 7) and pauses between consecutive attacks. We find that combining these parameters provides an improved demarcation between simple sequences of DDoS attacks, and more homogeneous pulse-wave patterns (see Figure 11). We tune these parameters by visual inspection of the results of the detected pulsed DDoS attacks and find our optima for the ratio between the mean and average durations to be lower than 1.5, and the entropy of the series of the durations to be lower than 2. Additionally, we require the entropy of the series of pauses between attacks to be less than 3.5 Finally, we require a repetitive DDoS event to be a candidate for a pulse-wave DDoS to have a sequence of at least 6 repetitive DDoS attacks.

VI. Characterizing Pulsed Attacks

A. General DDoS Characteristics

The first step of our approach (see § V-A) identifies 10,332 DDoS attacks with 17,219,000 flows to 2,901 individual

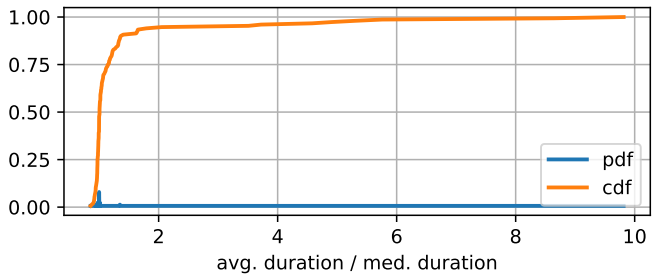


Fig. 6: Average duration / median duration of consecutive attack patterns used to identify pulse-wave patterns to differentiate them from simple sequences of DDoS attacks.

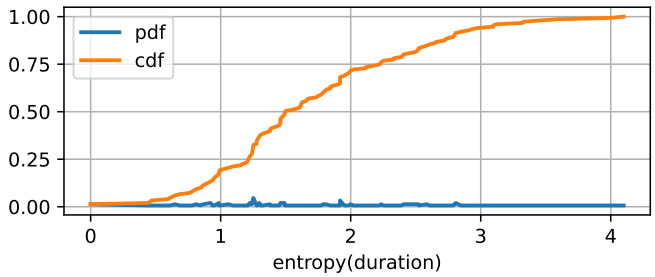


Fig. 7: Entropy of the sequence of durations of consecutive attack patterns used to identify pulse-wave patterns to differentiate them from simple sequences of DDoS attacks.

targets. Once we expand this initial view to our detected DDoS attacks, we arrive at 90,874,000 flows, an increase of 5.3. If we apply our identification of pulse-wave DDoS events (§ V-E) to the initial data set, we would only find 50 cases for pulse-wave DDoS events (half of our final results) but with a potentially high rate of false pulse-wave DDoS events.

Influence of Route Flappings. We are next interested in studying the influence of BGP route flapping. By combining the view of BGP update activity with potential pulse-wave DDoS events, we find only four cases where both activity patterns match. We show two examples of an overlay of BGP activity with pulse-wave DDoS events in Figure 8, where (a) shows a pulse-wave DDoS pattern with dissimilar BGP activity and (b) a consistent pattern of DDoS attacks and BGP updates. As we are interested in ruling out any potential false pulse-wave DDoS patterns, we omit samples with overlapping patterns of attacks and BGP updates.

Reoccurring DDoS attacks. In preparation for characterizing pulse-wave attacks, we look at the general repetition of DDoS attacks. As a basis, we define consecutive DDoS attacks as the series of reoccurring attacks towards the same target within one day. From our dataset, we can exclude 2,597 targets that were only exposed to a single attack per day and continue our analysis with 7,935 attacks on recurring targets. Thus, attacks with recurring targets represent 77% of all attacks in our data set. The maximum in our data set is 300-450 attack repetitions within a single day, which occurred 4 times.

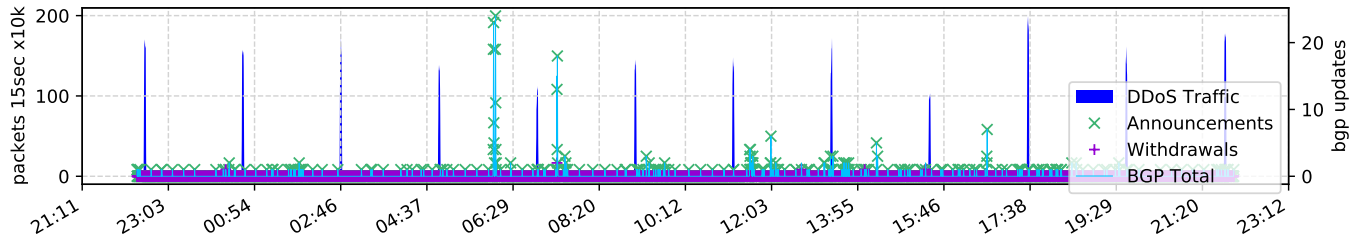
At this point, an investigation of the data set of reoccurring DDoS attacks can already provide interesting insights. In Figure 9, we examine the pauses between consecutive attacks. We show the time in seconds between repeated attacks towards the same target and with the same attack vector. The observed time frames span from a minimum of 15 seconds to a maximum of 6,400 seconds (1 day). We observe that short pauses occur most frequently. Additionally, notable steps are visible between 7,380 and 7,650, another step is located between 8,295 and 8,415, which points to homogeneous, potentially slow and long, pulsed DDoS attacks.

Furthermore, we look at the duration of individual attacks within a sequence of attack events in Figure 10. We find an apparent clustering at 60, 120, 150, and 195 seconds, with a long tail up to a maximum of 140,835 seconds (39h). Since our approach is capable of mapping a resolution of down to 15 seconds, the lower clusters are particularly interesting and indicate that the DDoS duration for repeated DDoS attacks is in the minute range, but also shows that DDoS attacks sub-minute are still uncommon and not to be expected for pulse-wave DDoS attacks in the wild.

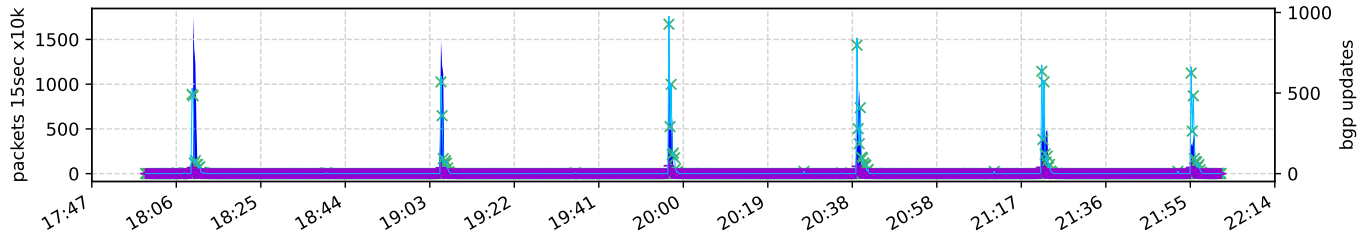
B. Pulse Wave DDoS Attacks

From the sequence of reoccurring DDoS attacks, we find pulse-wave DDoS events by applying the last step of our methodology § V-E, where we use different parameters of the duration of attacks and pauses between attacks. With this, we are able to separate simple repeated DDoS attacks against the same target from more homogeneous pulse-wave DDoS attacks. In Figure 11 we show exemplary events identified as pulse-wave DDoS and two events identified as not pulse-wave DDoS. The results show that our approach identifies pulse-wave DDoS events with different characteristics. Figure 11 (a) is a short pulse DDoS event, spanning 22 minutes, with a pulse duration of 1 minute. Figure 11 (b) depicts a pulse-wave DDoS event spanning over more than half a day, with only 6 short DDoS pulses. In contrast, Figures 11 (c) and (d) show two sequences of DDoS attacks, which are not identified as pulse-wave DDoS. From a visual appearance, it seems trivial to the reader to tell that both events show a pattern different from the identified pulse-wave events. However, with the unknown time frame, zoom factor, and resolution, the investigation of pulse-wave and consecutive DDoS events becomes challenging, even with a manual approach. Therefore, this measurement approach is highly beneficial in finding pulse-wave DDoS attacks and describing the landscape of reoccurring and pulse-wave DDoS attacks.

Table III gives an overview to compare the characteristics of different repetitions of DDoS attacks against the same target compared to pulse-wave events. From all attacks in our data set, we find 2,870 attacks to be associated with pulse-wave DDoS patterns, which comprises 27% of all attacks in our data set. This number of attacks folds into 102 events of pulse-wave DDoS, which have been targeted against 41 individual victims. Within the 102 pulse-wave DDoS events we find that the majority of attacks employ a long-pause pulse-



(a) Sample with no overlap of DDoS attack and BGP updates.



(b) Sample with strong overlap of BGP updates and DDoS attack pattern.

Fig. 8: Combining the DDoS attack traffic with the view on BGP updates.

				pulse (sec.)		pause (sec.)			
attacks	events	attacks	targets	avg.	med.	avg.	med.	Gbps	top 3 attack vectors
1	2597	2597	1953	269.99	60	-	-	101.75	DNS (95%), NTP (3%), SADP (0.38%)
2 - 5	550	1394	388	540.72	25	5867	337	98.22	DNS (81%), NTP (11.48%), SADP (2.15%)
>5	151	3671	63	658.13	180	5424	3345	73.39	DNS (96%), NTP (1.17%), SSDP (1.1%)
pulse-wave	102	2870	41	151.55	195	6207	5992	17.57	DNS (99.2%), SSDP (0.24%), SADP (0.21%)

TABLE III: Comparing different types of pulse-wave DDoS and consecutive DDoS attacks.

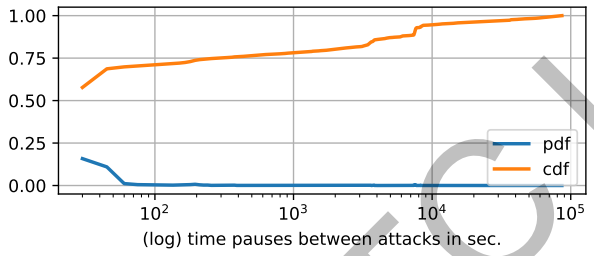


Fig. 9: Time between attacks from reoccurring DDoS against the same target.

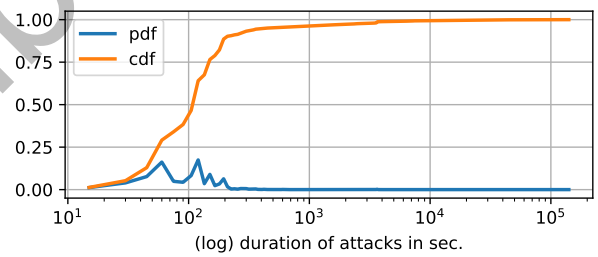
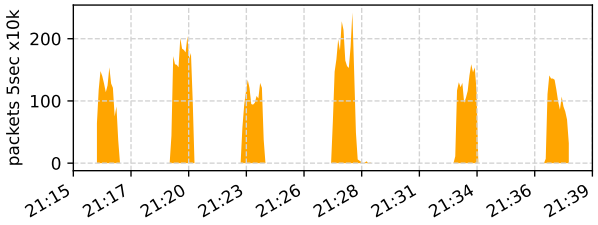


Fig. 10: Duration of attacks from reoccurring DDoS attacks against the same target.

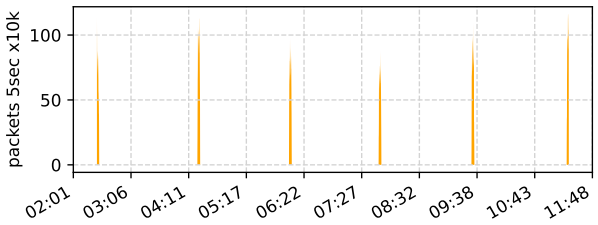
wave pattern, as shown in Figure 11 (b). Where the average pause between attacks leans towards 100 minutes. Comparing reoccurring DDoS attacks to pulse-wave DDoS, we notice that the average duration of pulses lowers significantly (from 658 to 151 seconds) towards pulse-wave DDoS events, as well as the maximum Gbps from 73.39 to 17.57 Gbps. When examining the amplification protocols employed, we observe a significant prevalence of DNS as the primary attack vector in pulse-wave DDoS events (99.2%), with SSDP ranking as the second most prominent attack vector, in contrast to NTP in non-pulse-wave DDoS attacks. In general, we see classical DDoS amplification protocols [11] to be used the most within pulse-wave DDoS events, but we also note that SADP occurs as an unexpected and potentially rising DDoS attack vector, similarly employed within pulse-wave DDoS events.

As previously mentioned, pulse-wave DDoS attacks are occasionally reported by industry reports (e.g., [50]), and research on theoretical aspects of DDoS mitigation exists. However, within the area of Internet measurements, there seems to be uncertainty about the prevalence and significance of consecutive and pulse-wave DDoS attacks. To answer this question, we provide a view on the occurrence and repetitions of DDoS attacks against specific targets in Figure 12.

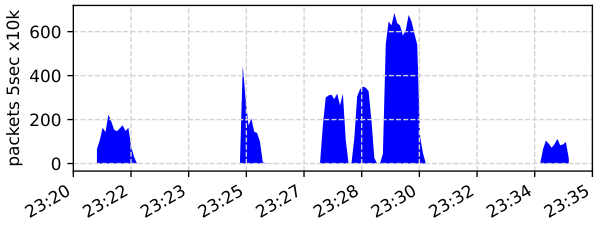
We group attack events by the count of reoccurring attacks against a specific target and additionally indicate the share of pulse-wave DDoS and non pulse-wave DDoS events. Figure 12 (a) depicts the count of the occurrence of attack events with specific amounts of repetitive attacks. Here, we



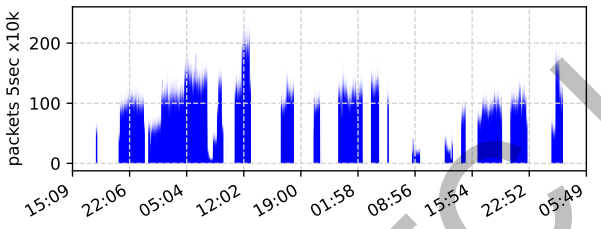
(a) Short pulse-wave attack pattern.



(b) Long pulse-wave attack pattern.

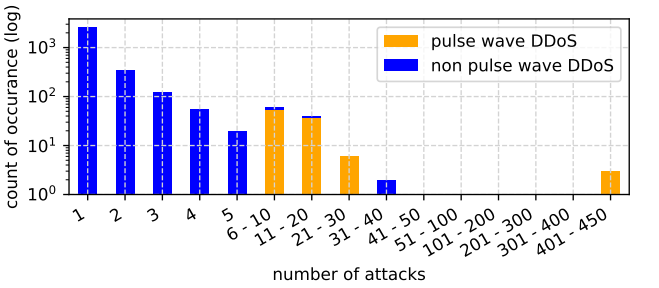


(c) Consecutive attacks, no pulse-wave pattern

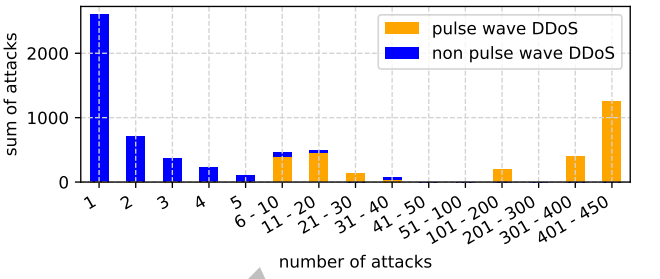


(d) Consecutive attacks, no pulse-wave pattern.

Fig. 11: Different types of pulse-wave and consecutive DDoS.



(a) Count of occurance of attacks with different number of individual attacks.



(b) Sum of attacks from events with different number of individual attacks.

Fig. 12: Attack repetitions against individual targets.

can see that the events of pulse-wave attacks are low, with 60 to 70 events composed of 6-10 or 11 to 20 individual attacks and fewer than 10 occurrences of attacks that included more than 20 individual attacks. From this perspective, pulse-wave DDoS attacks seem irrelevant compared to 2,597 occurrences of one-off attacks. However, this perception changes if we look at Figure 12 (b). Here, we summarize the attacks within each bucket. Therefore, we consider how many attacks a pulse-wave DDoS attack constitutes. Looking at the resulting distribution, we see that from the perception of individual DDoS attacks, the number of DDoS attacks attributed to pulse-wave DDoS attacks counters one-off attacks. Comparing Figure 12 (a) and (b) shows that a small number of pulse-wave DDoS events represents a large number of attacks. This underscores the importance for reporting on DDoS attack, but also for providing more effective DDoS detection and mitigation solutions. It shows that statistics on DDoS attacks can look significantly different when representing individual attacks or when considering pulse-wave DDoS events.

VII. Conclusion

In this study, we assessed the characteristics and extent of pulse-wave DDoS attacks in the wild. We proposed and implemented an approach to identify DDoS attack campaigns with pulse-wave patterns that have not been described in any Internet measurement study to date. Observing the landscape of DDoS attacks from the vantage point of a large IXP, we discover that pulsed DDoS attacks constitute 27% of individual DDoS attacks. We identified 102 DDoS pulsed attack events, which are characterized by consistent pulse-wave patterns, suggesting some degree of attack automation compared to consecutive or other repetitive DDoS attack events. We find that pulsed DDoS attacks have emerged as a significant attack tactic. This has direct implications for Internet measurement studies, which will overestimate the number of attack campaigns if they only count individual attacks instead of accounting for campaigns. Awareness about this attack type should be included in related measurement endeavors on DDoS, e.g., by using honeypots and Internet telescopes and observing DDoS attacks from botnets. We hope these findings on the repetitiveness and characteristics of pulsed DDoS attacks in the wild will guide future efforts to mitigate and measure DDoS attacks.

Acknowlegements. This work received funding by the Deutsche Forschungsgemeinschaft (DFG) as part of SPP 2378 (Resilient Worlds) project ReNO (grant number 511099228).

REFERENCES

[1] Akamai, "2018 State of the Internet / Security: A Year in Review," https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2018-state-of-the-internet-security-a-year-in-review.pdf, 2018.

[2] ZDNet, "GitHub hit with the largest DDoS attack ever seen," https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/, 2018.

[3] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti, "Millions of targets under attack: a macroscopic characterization of the DoS ecosystem," in *ACM IMC*, 2017.

[4] R. Hiesgen, M. Nawrocki, M. Barcellos, D. Kopp, O. Hohlfeld, E. Chan, R. Dobbins, C. Doerr, C. Rossow, D. R. Thomas, M. Jonker, R. Mok, X. Luo, J. Kristoff, T. C. Schmidt, M. Wählisch, and k. claffy, "The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments," in *ACM IMC*, 2024.

[5] N. Y. Times, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool," https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html, 2017.

[6] A. Büscher and T. Holz, "Tracking DDoS Attacks: Insights into the Business of Disrupting the Web," in *USENIX Workshop on Large-Scale Exploits and Emergent Threats*, 2012.

[7] J. Mohamed, "Daily Mirror: Hackers attack the Stock Exchange: Cyber criminals take down website for more than two hours as part of protest against world's banks," http://www.dailymail.co.uk/news/article-3625656/Hackers-attack-Stock-Exchange-Cyber-criminals-website-two-hours-protest-against-world-s-banks.html, 2016.

[8] BBC, "'Hacking attacks' hit Russian political sites," http://www.bbc.com/news/technology-16032402, 2012.

[9] I. Traynor, "Russia accused of unleashing cyberwar to disable Estonia," https://www.theguardian.com/world/2007/may/17/topstories3.russia, 2007.

[10] Interfax-Ukraine, "Poroshenko reports on DDoS-attacks on Ukrainian CEC from Russia on Feb. 24-25," https://www.kyivpost.com/ukraine-politics/poroshenko-reports-on-ddos-attacks-on-ukrainian-cec-from-russia-on-feb-24-25.html, 2019.

[11] D. Kopp, C. Dietzel, and O. Hohlfeld, "DDoS never dies? an IXP perspective on DDoS amplification attacks," in *PAM*, 2021.

[12] D. Kopp, M. Wichtlhuber, I. Poese, J. J. C. de Santanna, O. Hohlfeld, and C. Dietzel, "DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown," in *ACM IMC*, 2019.

[13] A. Toh, "Azure DDoS Protection—2021 Q3 and Q4 DDoS Attack Trends," https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/, 2022.

[14] A. S. Alerts. (2018) Memcached-fueled 1.3 tbps attacks. https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html.

[15] T. Greene, "How the Dyn DDoS Attack Unfolded," https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html, 2016.

[16] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," *NDSS*, 2014.

[17] M. Wichtlhuber, E. Strehle, L. Prepens, A. Rubina, D. K. p, S. Stegmüller, C. Dietzel, and O. Hohlfeld, "IXP Scrubber: Learning from Blackholing Traffic for ML-Driven DDoS Detection at Scale," in *ACM SIGCOMM*, 2022, p. 707–722.

[18] Akamai, "Prolexic Technologies by Akamai," https://www.akamai.com/us/en/cloud-security.jsp, 2018.

[19] D. Gillman, Y. Lin, B. Maggs, and R. K. Sitaraman, "Protecting Websites from Attack with Secure Delivery Networks," *IEEE Computer Magazine*, vol. 48-4, 2015.

[20] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, "Measuring the Adoption of DDoS Protection Services," in *ACM IMC*, 2016.

[21] T. Vissers, T. V. Goethem, W. Joosen, and N. Nikiforakis, "Maneuvering around Clouds: Bypassing cloud-based Security Providers," *ACM CCS*, 2015.

[22] G. C. M. Moura, C. Hesselman, G. Schaapman, N. Boerman, and O. de Weerdt, "Into the DDoS maelstrom: a longitudinal study of a scrubbing service," in *Euro S&P Workshops*, 2020.

[23] C. Dietzel, A. Feldmann, and T. King, "Blackholing at IXPs: On the Effectiveness of DDoS Mitigation in the Wild," *PAM*, 2016.

[24] C. Dietzel, M. Wichtlhuber, G. Smaragdakis, and A. Feldmann, "Stellar: Network Attack Mitigation using Advanced Blackholing," in *ACM CoNEXT*, 2018.

[25] M. Jonker, A. Pras, A. Dainotti, and A. Sperotto, "A First Joint Look at DoS Atacks and BGP Blackholing in the Wild," in *ACM IMC*, 2018.

[26] A. G. Alcoz, M. Strohmeier, V. Lenders, and L. Vanbever, "Aggregate-based congestion control for pulse-wave ddos defense," in *ACM SIGCOMM*, 2022.

[27] J. Park, D. Nyang, and A. Mohaisen, "Timing is almost everything: Realistic evaluation of the very short intermittent ddos attacks," in *Annual Conference on Privacy, Security and Trust*, 2018.

[28] R. Guo, J. Chen, Y. Wang, K. Mu, B. Liu, X. Li, C. Zhang, H. Duan, and J. Wu, "Temporal CDN-Convex lens: A CDN-Assisted practical pulsing DDoS attack," in *USENIX Security Symposium*, 2023.

[29] Y.-M. Ke, C.-W. Chen, H.-C. Hsiao, A. Perrig, and V. Sekar, "Cicadas: Congesting the internet with coordinated and decentralized pulsating attacks," in *AsiaCCS*, 2016.

[30] X. Luo and R. K. C. Chang, "On a new class of pulsing denial-of-service attacks and the defense," 2005.

[31] R. Rasti, M. Murthy, N. Weaver, and V. Paxson, "Temporal lensing and its application in pulsing denial-of-service attacks," in *IEEE Symposium on Security and Privacy*, 2015.

[32] M. Prince, "The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)," https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/, 2013.

[33] ——, "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack," https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/, 2014.

[34] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," *USENIX Security Symposium*, 2017.

[35] B. Krebs, "KrebsOnSecurity Hit With Record DDoS," https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos, 2016.

[36] F. Lichtblau, F. Streibelt, T. Krüger, P. Richter, and A. Feldmann, "Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses," in *ACM IMC*, 2017.

[37] R. Beverly, A. Berger, Y. Hyun, and k. claffy, "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering," in *ACM IMC*, 2009.

[38] R. Beverly and S. Bauer, "The spoofer project: Inferring the extent of internet source address filtering on the internet," in *Steps to Reducing Unwanted Traffic on the Internet Workshop*, 2005.

[39] D. Moore, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," in *USENIX Security Symposium*, 2001.

[40] M. Luckie, R. Beverly, R. Koga, K. Keys, J. A. Kroll, and k. claffy, "Network hygiene, incentives, and regulation: Deployment of source address validation in the internet," in *CCS*, 2019.

[41] US-CERT, "UDP-Based Amplification Attacks," https://www.us-cert.gov/ncas/alerts/TA14-017A, 2018.

[42] F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and DRDoS Attack Defense–A Survey and New Perspectives," *arXiv preprint arXiv:1505.07892*, 2015.

[43] Akamai, "State of the Internet Security Report," https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-attack-spotlight.pdf, 2018.

[44] C. Morales, "Netsout Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us," https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/, 2018.

[45] D. Wagner, D. Kopp, M. Wichtlhuber, C. Dietzel, O. Hohlfeld, G. Smaragdakis, and A. Feldmann, "United we stand: Collaborative detection and mitigation of amplification ddos attacks at scale," in *CCS*, 2021.

[46] R. Singh Samra and M. Barcellos, "Ddos2vec: Flow-level characterisation of volumetric ddos attacks at scale," in *ACM CoNEXT*, 2022.

[47] Nokia, "Filter Policies," 2020, accessed: 2020-05-24. [Online]. Available: https://documentation.nokia.com/html/0_add-h-f/93-0073-HTML/7750_SR_OS_Router_Configuration_Guide/filters.html

[48] Cisco, "Impl. BGP Flowspec," https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html, 2018.

[49] T. King, C. Dietzel, J. Snijders, G. Doering, and G. Hankins, "BLACKHOLE Community," IETF RFC 7999, 2016.

[50] Imperva, "Attackers Use DDoS Pulses to Pin Down Multiple Targets," https://www.imperva.com/blog/archive/pulse-wave-ddos-pins-down-multiple-targets/, 2016.