Universiteit van Amsterdam

Research Project II

DDoS Defense Mechanisms for IXP Infrastructures

July 13, 2018

Lennart van Gijtenbeek
System and Network Engineering
lennart.vangijtenbeek@os3.nl

Tim Dijkhuizen
Security and Network Engineering
tim.dijkhuizen@os3.nl

Supervisor
Stavros Konstantaras
Amsterdam Internet Exchange (AMS-IX)
stavros.konstantaras@ams-ix.net

Abstract

Distributed Denial of Service (DDoS) attacks are a serious threat to the Internet since they cause vital services to become unavailable. Their frequency, magnitude, and complexity has increased in recent years. This may be attributed to the fact that DDoS-as-a-service systems are provided online at low cost. AMS-IX wants to investigate if their central position as an IXP can be used to provide an on-demand DDoS defense service to its customers. Such a construction comes with numerous challenges since IXPs traditionally do not interfere in the exchange of traffic. Furthermore, the IXP environment has many possible ingress locations for DDoS attacks and exchanges large amounts of traffic. This complicates the identification process of the defense mechanism. This research defines several defense principles that take into account the restrictions that come with the IXP environment. This paper proposes a design for a DDoS defense mechanism that is applicable to IXP infrastructures in general. The design makes use of the underlying technical infrastructure seen in IXPs nowadays, such as route servers, access switches, and statistics collectors. The administrator of the victim AS initiates the detection and mitigation process. The identification phase of the design uses a threshold-based detection technique to determine the prefix under attack. The source ASes involved in the attack are identified, after which appropriate mitigation methods are applied. A two-way mitigation approach is taken by announcing a BGP blackhole next-hop to the source AS or configuring a layer 2 ACL on the ingress switch. By means of a proof of concept, the interaction between the components used in the proposed design is tested. Scalability of the design should be taken into consideration and therefore future work should be performed that examines the applicability of the design in an IXP environment.

Contents

1 Introduction **1**
- 1.1 Research questions . . . 1
- 1.2 Scope . . . 2
- 1.3 Ethical considerations . . . 2
- 1.4 Contributions . . . 2
- 1.5 Overview . . . 2

2 Background **2**
- 2.1 IXP networks . . . 2
  - 2.1.1 Route servers . . . 3
  - 2.1.2 AMS-IX . . . 3
- 2.2 DDoS . . . 4
  - 2.2.1 Attack infrastructures . . . 4
  - 2.2.2 Types of DDoS attacks . . . 4
- 2.3 Identification and mitigation . . . 5
  - 2.3.1 Traffic monitoring . . . 6
  - 2.3.2 Detection methods . . . 6
  - 2.3.3 Mitigation methods . . . 7
- 2.4 Related work . . . 8

3 Development Constraints **9**
- 3.1 Design restrictions . . . 9
- 3.2 Defense principles . . . 9

4 Two-way Mitigation Design **10**
- 4.1 Identification and mitigation decisions . . . 10
- 4.2 Design workflow . . . 11
- 4.3 Architecture . . . 12
- 4.4 Mitigation overview . . . 14
- 4.5 Phase workflows . . . 14
  - 4.5.1 Identification phase . . . 14
  - 4.5.2 Mitigation decision phase . . . 15
  - 4.5.3 Blackhole next-hop mitigation phase . . . 16
  - 4.5.4 Ingress layer 2 ACL mitigation phase . . . 17

5 Experimentation **18**
- 5.1 Experimental setup . . . 18
- 5.2 Testing scenarios . . . 20
- 5.3 Results . . . 20
  - 5.3.1 Scenario 1 . . . 20
  - 5.3.2 Scenario 2 . . . 21
  - 5.3.3 Scenario 3 . . . 21

6 Discussion **22**

7 Conclusion **23**

8 Future Work **23**

9 Acknowledgements **24**

References **25**

1 Introduction

Internet eXchange Points (IXPs) play a significant role in the modern Internet era by transferring bits in a more efficient and cost-effective way. As a result of this, parties establish interconnections at IXPs to peer with each other over BGP. At the start of 2018, several Distributed Denial of Service (DDoS) attacks occurred in the Netherlands that were aimed at vital infrastructures [26]. There is an increased need from the AMS-IX peering community to look into this problem [53]. Therefore, AMS-IX is interested in providing an on-demand DDoS mitigation service to its customers. There is currently no identification or mitigation mechanism active within the AMS-IX network. In case of DDoS attacks, AMS-IX currently allows for re-routing to the Nationale Wastraat (NaWas) scrubbing center over its network or blocks customer ports on request [45]. Also, the Trusted Networks Initiative (TNI) has been introduced by AMS-IX to relieve the issues [5].

DDoS attacks are a serious threat on the Internet and continue to increase in frequency, size and complexity [14, 48, 49, 58]. DDoS attacks cause vital Internet services to become unavailable for extended periods of time. This is why these attacks are considered one of the biggest security threats to date. The security of the general Internet is related to the state of DDoS. Systems that are subverted by malicious software are often involved in DDoS attacks. These systems form botnets that are used to perform DDoS attacks. Booter services can be rented online and effectively allow its customers without technical knowledge to perform DDoS attacks at low monetary cost [50].

The infrastructure making up the global Internet is distributed among many administrative domains. It is therefore not an easy task to implement a global policy to combat DDoS attacks. The effectiveness of the Internet is mainly focused on transferring packets from source to destination. The Internet is set up following the end-to-end principle; the intelligence resides in the edge of the network and not in the core of the network. The core of the network by design limits itself to the lower layers of the OSI model to perform routing and forwarding [61]. By default, there is no policing done and senders can misbehave and perform attacks on their destination without the network interfering. Functions such as reliable transport and security are left to the end hosts to implement. Two unfortunate implications are IP spoofing and DDoS attacks. Using IP spoofing, the DDoS attacker can escape accountability and detection. Furthermore, reflection attacks arise because IPs can be spoofed [48].

IP spoofing and open resolvers are two of the main issues relating to Internet security to date. If all Internet connectivity providers implemented network ingress filtering on their network, IP spoofing would no longer be an issue [23]. Similar results can be achieved by implementing Unicast Reverse Path Forwarding (uRPF) [6]. This would effectively combat all DDoS attacks that make use of IP spoofing. Open resolvers are another issue; these machines are abused in reflection attacks to generate huge amounts of data. The open resolvers are misconfigured to accept connections from outside networks and thereby become involved in DDoS attacks.

Since IXPs interconnect many Autonomous Systems (ASes), they have a central position with respect to these networks. IXPs provide a vantage point with an excellent view over the global Internet [11]. In our research, this vantage point can be used for detection and mitigation of DDoS attacks by being able to look at traffic at an inter-domain level. If a customer AS connected to the IXP environment does not have a mitigation solution, they will benefit from the IXP implementing such a mechanism.

DDoS defense inside the IXP network comes with numerous challenges. Firstly, the traffic load on the network is high. This requires efficient monitoring of traffic and an effective detection method. Secondly, the IXP environment is a neutral environment that functions as a large layer 2 switch. The IXP must be careful on how to mitigate with respect to blocking and filtering traffic. For example, should the IXP implement methods to detect IP spoofing, or not look into source-based filtering at all? IXPs adhere to the end-to-end principle and do not interfere in the customer's traffic. Since the IXP's customers can be competitors, it is important for IXPs to be a neutral entity. This is what makes DDoS defense in the IXP network an interesting, but challenging subject. Thirdly, the IXP network is a complex environment with many possible ingress and egress points for DDoS attacks, since numerous networks are interconnected. This brings up challenges with respect to the scalability of the solution.

1.1 Research questions

Following from the introduction, our research question is defined as:

- What (automated on-demand) solution can be developed to defend against DDoS attacks in an IXP network?

In order to answer our main research question, the following sub-questions are defined with respect to IXP environments:

- What detection mechanisms exist or can be developed to identify DDoS attacks?
- What mechanisms exist or can be developed to mitigate DDoS attacks?

- How can the above mechanisms be combined efficiently into an IXP compatible defense mechanism?

1.2 Scope

This research focuses on creating a design proposal for a DDoS defense mechanism that can be applied in IXP infrastructures. We investigate into the AMS-IX network as our base point. The amount of different DDoS attacks is plenteous [33]. Therefore, we do not aim to detect all of these specific attacks but focus on detecting the most prevalent classes of attacks. An experimentation environment is set up to test the interaction between the components in the design. This setup does not test all of the optimization and scalability aspects of the design.

1.3 Ethical considerations

Large amounts of private data traverses the IXP network on a daily basis. While conducting this research, the privacy of the end-users is kept in mind. An IXP does not do any layer 3 routing between connected parties and only looks into layer 2 headers to forward traffic. For DDoS identification purposes, we found that it was required to look into layer 3 headers of packets. Whether or not such a solution is acceptable to the AMS-IX peering community, is up for debate.

1.4 Contributions

IXP infrastructures throughout Europe have proven to be similar with respect to their underlying technologies [2]. We propose a two-way mitigation design against DDoS attacks for IXP environments. For the identification and mitigating process, we have focused on using the available infrastructure that IXPs already adopt. Our design workflow is split up into four phases and uses two types of mitigation methods depending on the situation. The DDoS Threat Mitigator (DTM) queries the statistics collector, which is already present in the AMS-IX environment for traffic monitoring purposes. The DTM makes use of threshold-based detection to identify attacks. This is done by means of a DDoS Threshold Adviser (DTA) and a Current Traffic Analyzer (CTA). We focus on detecting volumetric attacks and protocol attacks by using bits per second and packets per second as metrics. Our solution makes use of layer 2 Access Control Lists (ACLs) and does not require any layer 3 packet analysis on the ingress switches when the traffic is filtered. This is done with respect to adapting to the IXP environment and effectively allowing the IXP to keep functioning as a big layer 2 switch. We tested the interaction between the components used in the design by means of a proof of concept.

1.5 Overview

The DDoS field is large and extensive research has been done into the subject. Therefore, we start this paper with a background section to get the reader up to date on the current developments. The background section is vital to understand the reasoning that is applied in the rest of the paper. The section following the background (section 3) focuses on the constraints we face and the principles we found important to adhere to while constructing our design. In section 4, we discuss the design proposal and how the decisions to come to this construction were made. Section 5 focuses on the experimentation phase of our study, where we explain the proof of concept that we implemented and provide the results of several testing scenarios. Following this section, we present the discussion, conclusion and future work sections.

2 Background

In this background section, we provide information on the infrastructure of IXP networks and different types of DDoS attacks.

2.1 IXP networks

In the modern Internet, IXP networks have arisen to facilitate the local exchange of traffic between Autonomous Systems (ASes). In the IXP environment, ASes peer via the Border Gateway Protocol (BGP) to perform inter-AS routing, by means of advertising their IP prefixes. Transit providers commonly charge for traffic on a per bit basis which is why sending traffic to direct peers is preferred. This also causes the traffic to take a shorter route and therefore the latency is decreased. Another advantage is that the IXP adds redundancy. Customer networks connect their BGP border router(s) to an access switch on the IXP network. These routers are referred to as Customer Edge (CE) routers. ASes still have their transit provider set as the default gateway for non-local traffic destined for the global Internet.

BGP peering parties need to be directly connected since External BGP (eBGP) protocol packets use a TTL of 1 (network layer) [34]. The IXP infrastructure can be abstracted as a single LAN on which parties exchange traffic on layer 2 of the OSI model [61]. Therefore, IP routing information is not needed to forward packets that are inserted into the IXP network. Peerings are set up manually since BGP routing involves policy and politics and therefore dynamic neighbor discovery (as in IGPs) is unwanted. Route servers are an exception to this, which we will further discuss in section 2.1.1.

In the general case, the peering LAN is not used for transit traffic. This means that parties do not route each other's traffic. However, there may be exceptions to this rule. Please note that the term 'BGP peering' is broad and indicates setting up a BGP session between two parties; it does not always mean settlement-free peering.

2.1.1 Route servers

Open peering is defined as the process in which a single AS peers with all other ASes on the IXP network. Route servers are essential to scale the BGP sessions to achieve open peering. Through the use of route servers, AS border routers can simply peer with the route server, instead of individually peering with all the other ASes. This reduces the number of BGP connections that the customers have to manage. Customers can still manage their most important peer privately. The route server runs BGP speaker software, and stores all the prefixes announced by the ASes it peers with [47]. Consequently, it performs ingress filtering and egress filtering, before it propagates its route database to the connected border routers. Route servers do not prepend their own AS number to the AS path. This means that the connected customers receive the announced prefixes as if they are directly connected to the BGP border router responsible for the announcement. The route server is not part of the forwarding path.

2.1.2 AMS-IX

AMS-IX has approximately 820 peers, of which around 700 peers engage in peering with the route server. AMS-IX has access switches in multiple data centers around Amsterdam. For redundancy purposes, AMS-IX has two route servers, which run BIRD as the BGP routing daemon. Each day the peak traffic exchange rate is around 5,6 Tbps [4]. AMS-IX currently allows customers to disable access switch port(s) or route traffic to the Nationale Wastraat (NaWas) scrubbing center, to relieve themselves of DDoS attacks. The CE routers connected to the AMS-IX access switches are assigned an IP address in the AMS-IX subnet. IRRdb [31] and RPKI validator [39] are used on the route server in outbound filtering.

The traffic forwarding on the peering LAN is done via layer 2 Multi-Protocol Label Switching (MPLS). The access switches (Provider Edge (PE) routers) function as MPLS label edge routers (LERs). The ingress LER will push an MPLS label on the packets inserted in the AMS-IX network. This is done to forward the packets over predefined label switched paths (LSPs), corresponding to the destination MAC address. The LSPs, also known as pseudowires, are set up using RSVP-TE in a full mesh between all the PE routers. This setup is chosen since it allows for redundant paths and load balancing over the core switches. The main peering LAN is implemented with Virtual Private LAN Service (VPLS), on top of the MPLS LSPs. A complete overview of the AMS-IX topology can be found in figure 1.

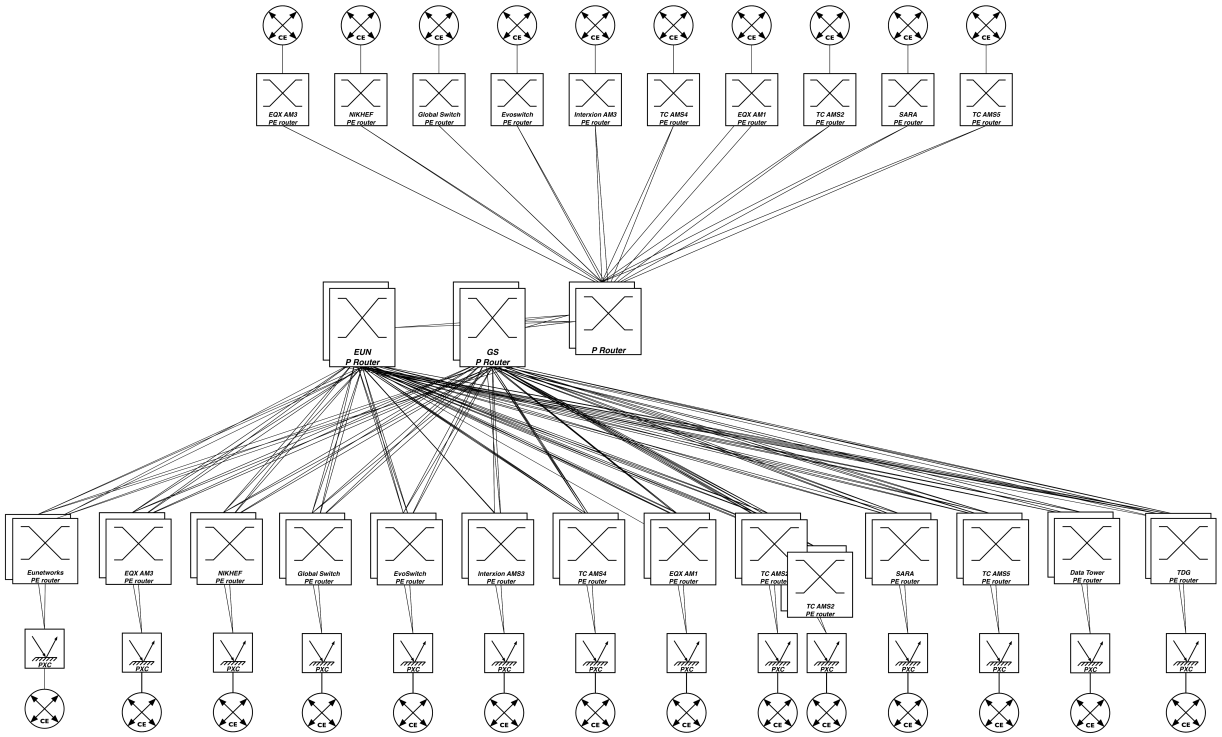

Figure 1: AMS-IX infrastructure [3]

2.2 DDoS

In this section, we discuss the infrastructure responsible for the generation of DDoS attack traffic and the types of DDoS attacks commonly executed.

2.2.1 Attack infrastructures

In order to launch DDoS attacks, the attacker coordinates a set of machines. Often, botnets are used to launch DDoS attacks [36]. These botnets are set up by infecting vulnerable (Internet-facing) machines with malware. The malware runs in the background and communicates with the command and control (C&C) machine of the attacker. The C&C machine is used to issue commands to the bots. When a DDoS attack originates from multiple bots, the attack is harder to block from a defender's perspective, since the sources may appear as legitimate devices. Attacks can also be executed from a set of rented Virtual Private Servers (VPSs). Increasingly, DDoS attacks are provided as a service online. These types of DDoS infrastructures are known as booters, stressers, or DDoS-as-a-Service [50]. New botnets have been observed in the wild that predominantly contain infected IoT devices. Commonly, IoT devices do not have strong security features and can often be infected with malware more easily than traditional Internet-facing devices [57]. An example of a successful attempt at exploiting IoT devices in order to perform DDoS attacks is the Mirai botnet in 2016 [28].

2.2.2 Types of DDoS attacks

In order to identify and mitigate DDoS attacks, it is advantageous to understand the characteristics of the attacks. There are a wide variety of DDoS attacks, which each work in different ways. This is a challenge when defending against DDoS attacks since there is no single detection method for all of these attacks. In this section, we explain the different classes of DDoS attacks that exist today and discuss an example attack for each of these classes. DDoS attacks can either be direct or reflected. In the case of a reflected attack, IP spoofing is a requirement for the attack to succeed. In case of direct attacks, IP spoofing can optionally be used for the attacker's machines to avoid detection. We categorize attacks in the following four categories: volumetric, amplification, protocol, and application attacks. Note that amplification attacks are a subclass of volumetric attacks. In volumetric and amplification attacks, an overwhelming amount of data is sent to the victim in order to exhaust the network and/or server's resources. Protocol and application attacks are more refined and abuse

servers to exhaust their state or computational resources. The main difference between amplification attacks and protocol attacks is that amplification attacks send large packets that take up a lot of bandwidth, whereas protocol attacks send a lot of small packets. For each of these attacks, we also briefly discuss methods that can be used to mitigate it at the destination network. Since our mitigation research looks into techniques to mitigate at the IXP level, these are mostly not applicable for our study.

Volumetric attacks
The main objective of volumetric attacks is to send a lot of traffic in a 'dumb' manner to congest the network bandwidth between the victim and the Internet or exhaust its computational resources [59]. Since these attacks leave a large footprint with respect to bandwidth they are most easy to identify and mitigate. A common volumetric attack is the UDP flood. In this attack, various ports are flooded with UDP traffic. This forces the destination to check if there is a program running at the destination port; if nothing is running, it will send an *ICMP Not Reachable* message back. It is possible to overwhelm the target machine since this response process requires resources. It is likely that the firewall will become the bottleneck in this type of attack since it has to process a large amount of traffic. This type of attack can be mitigated at the destination by limiting the amount of ICMP responses; however, this also affects good traffic.

Amplification attacks
These types of attacks are also known as Distributed Reflection Denial of Service (DRDoS) attacks. In DRDoS attacks, open resolvers (the reflectors) are targeted with a load of UDP requests with spoofed source IP addresses of a target machine [49]. This causes the open resolvers to direct their responses to the queries to the victim machine(s). In essence, small requests create larger responses, which means a higher amount of traffic can be generated with fewer attack machines. Examples of protocols used for amplification attacks are DNS, DNSSEC, NTP, SNMP, and Memcached [14, 48, 56]. When response packets exceed the link MTU, packets are fragmented and will need to be reassembled at the destination. Besides the fact that the amplification attack takes up a lot of bandwidth, this also puts a lot of load on the target's resources since it will have to reassemble the packets. If each ISP properly implemented IP spoofing filtering, these attacks would not be able to succeed [6, 23]. Besides that, DRDoS attacks would be harder to perform if open resolvers were not misconfigured to accept queries from everywhere without validating the source IPs.

Protocol attacks
State exhaustion attacks, also known as protocol attacks, abuse weaknesses in the layer 3 and layer 4 protocols to cause service disruptions on the victim. These attacks are based on consuming the available state table capacity on their target servers. The TCP SYN flood is an example of a protocol attack [18]. This attack exploits the three-way handshake in the TCP protocol. The attacker continuously sends SYN packets to the target server but never replies to the SYN/ACK packets the server responds with. This causes many half-open connections to be maintained by the server which fills up the TCP state table. These connections are only purged after a certain amount of time. In the case of direct attacks, the attacker needs some mechanism (e.g. firewall) to stop their TCP ACK to the server. These attacks can be addressed in several ways. In order to mitigate, it is possible to increase the number of TCP connections or recycle the oldest half-open connections to make room for new connections. More advanced methods are to use SYN cookies or install a high capacity proxy that handles the three-way handshake on behalf of your servers.

Application attacks
These type of attacks focus on exploiting application layer protocols. The goal is to saturate the computational resources with malicious requests, such that legitimate queries can no longer be handled by the targeted server. This attack can be harder to detect since the intermediate forwarding equipment by default does not inspect packets above the network layer. The HTTP request flood attack is an example of an application layer attack. HTTP flood attacks are hard to spot since they use standard URL requests, which makes it hard to distinguish bad traffic from good traffic. For application attacks, an example mitigation method is to implement a highly distributed system that spreads the queries over many data centers to share the load. One could also make use of Google's reCAPTCHA software to prevent bots performing actions in the case of HTTP attacks [25].

2.3 Identification and mitigation

In this background section, we discuss the several types of identification and mitigation methods that we have investigated. In our design phase, we reflect back on these methods and combine several approaches to come to the final result.

2.3.1 Traffic monitoring

In order to identify a DDoS attack, one has to look into the traffic to recognize any rogue traffic. Therefore, the monitoring of network traffic is the first step in the identification of a DDoS attack. The parameters usable in layer 2 analysis are limited. MAC addresses only identify the traffic between two directly connected machines, which is not enough information since DDoS attacks travel longer distances from source to destination. We find that other layer 2 metrics such as send rate, arrival interval, frame size, and the Cyclic Redundancy Check (CRC) are complex to use in the identification process. Layer 3 provides more promising possibilities since the IPv4 and IPv6 protocols can be analyzed. DDoS identification and mitigation decisions can be made based on the source and destination IP address. On layer 4 of the OSI model, additional header fields can provide more insight into the type of DDoS attacks. The source and destination port indicate the type of application protocol involved, and TCP flags (SYN, ACK, sequence number, acknowledgment number) can be monitored to analyze protocol attacks.

Port mirroring
Traffic can be monitored by means of setting up a spanning port on switches or routers [10]. This method will effectively mirror all of the traffic that traverses the device and send it out on the mirrored port. On the outgoing connection, a device can listen to analyze the monitored traffic. The advantage is that with this method all traffic is monitored. For high traffic loads, this may not be an option since analysis of all the traffic in real-time will require a lot of computational resources and hardware [1].

Packet capture engines
Similar to port mirroring, this method takes place on the switch and/or router. Several packet capture engines exist that continuously run on switches and analyze traffic based on flows [10, 43]. Common packet capture protocols are NetFlow [41], sFlow [43, 51], and IPFIX [13]. Ingress network devices capture the traffic and forward it in protocol format to a central statistics collector. On the AMS-IX platform, sFlow is used in this manner on the access switches, which registers OSI header information up to and including layer 4. Not all traffic needs to be forwarded to the statistics collector since sFlow/NetFlow can be configured with a certain sample and polling rate. The sample rate is the configuration of sampling 1/n amount of packets and the polling rate configures the number of seconds that the packets going through the sample agent have to be counted. At the statistics collector, the sampled packets are extrapolated in order to provide an approximation of the actual traffic.

2.3.2 Detection methods

There are multiple possible options to identify DDoS traffic. In our study, we focus on threshold-based detection. In this subsection, we also look into fingerprinting and artificial intelligence methods.

Threshold-based detection
In threshold-based detection, historical data is used to calculate thresholds based on certain metrics. Metrics such as bits per second (BPS) and packets per second (PPS) can be used at the network layer. On layer 4, more advanced metrics such as the number of TCP SYN packets and TCP ACK packets can be used to identify attacks more accurately. By analyzing current traffic flows towards a destination IP or group of destination IPs, it is possible to detect anomalies in traffic rates and traffic types. If current traffic exceeds a BPS threshold to a certain destination IP, it is likely that this destination is suffering from volumetric DDoS attack. By analyzing layer 4 headers of the traffic as well, it can become clear whether or not this is indeed the case (e.g. only a certain type of traffic). It is important that thresholds are to be determined over an extended period of time, such that traffic spikes are filtered out in the average. In the case of BPS and PPS, an additional percentage can be added to the average to calculate the thresholds. The advantage of this method is that it is straightforward. Another advantage of threshold-based detection is that if the thresholds are set accurately, false negatives for the most common DDoS attacks should be limited. Additionally, pattern matching methods can be implemented to also put thresholds on packets that share the same characteristics.

Fingerprinting
This technique allows for identification of DDoS attacks based on information of earlier attacks. By creating signatures of past attacks, live traffic can be analyzed and compared to these signatures in order to identify attacks. The DDoSDB project is an example project that uses this type of approach [54]. In the DDoSDB database, attack signatures are stored and used to identify future attacks. Signatures are mainly based upon source IPs, source ports, and destination ports. The advantage of this approach is that attacks can be analyzed in depth. However, attacks not seen in the wild before will be missed in this system and thus false negatives may occur if only this method is used. Still, this approach will prove advantageous to learn from past attacks

and to make mitigation decisions based upon the knowledge obtained. For example, IPs can be blacklisted that are often involved in DDoS attacks.

Artificial intelligence
DDoS attack detection can be implemented using artificial intelligence (AI) methods. Machine learning classification methods can be used to make a distinction between good and bad traffic. Mainly, AI methods such as neural networks, naive bayes, support vector machines (SVMs) and random trees are used for these purposes. We discuss more about AI research in DDoS defense in the related work section (section 2.4).

2.3.3 Mitigation methods

When defending against DDoS attacks, the most straightforward method is to scale up your network equipment and servers. Overprovisioning provides for more attack absorption and also creates additional time to react. Using load balancing and/or IP anycast diffusion to spread traffic over multiple data centers is another general method of defense. In this section, we focus on several different mitigation methods besides these more obvious approaches.

Scrubbing appliances
Scrubbers are all-in-one DDoS identification and mitigation appliances. These commercial solutions have custom-made network cards and hardware architectures to handle monitoring and mitigation at line rates. Thus, these appliances can be positioned inline on the regular forwarding path. The main focus of these appliances is to identify and drop the bad traffic while still allowing the good traffic to pass through. Several companies providing such solutions are Arbor [42], Radware [46] and Huawei [30].

Off-site scrubbing centers exist that can be used by networks that do not have their own on-site scrubbing appliance. The NaWas is a Dutch scrubbing center that is used for these purposes [45]. Networks can reroute their traffic to these off-site scrubbing centers via BGP announcements or DNS records (A/AAAA). BGP re-routing is the most comprehensive method since it works across all protocols. The scrubbing center can announce a more specific prefix of a customer network (on demand), such that the traffic is drawn there. After the traffic has been cleaned, it is re-routed back to the customer network to its original destination. Routing back to the customer network can be done using a Generic Routing Encapsulation (GRE) tunnel [19]. The advantages of scrubbers are that they only drop bad traffic (in case of no false positives), and can handle complex DDoS attacks. The disadvantages are that these boxes are expensive and proprietary. For off-site scrubbing, there is also BGP convergence time. Thus, the mitigation is not instantly applied and there is an increase in latency since the traffic has to be re-routed.

BGP announcements
Blackholing is a mitigation technique by which certain traffic on a switch or router is directed to a null interface. There are several ways of implementing blackholing via BGP announcements. A common approach used in IXPs is Remote Triggered Blackholing (RTBH); we explain more about this in the related work section (section 2.4). There are two types of blackholing via BGP: source-based blackholing and destination-based blackholing. Destination-based blackholing can be implemented in two ways.

In the first approach of destination-based blackholing, the upstream network where the DDoS originates from can be signaled such that traffic to the destination(s) under attack is either re-routed or dropped. This can be done by advertising a route withdrawal to the upstream or advertising a null route that is statically configured by the upstream on its border routers. In the first case, traffic will most likely find another route to the destination (in case of multi-homing) whereas in the second case the traffic is dropped. The null route can be advertised using a predefined blackholing IP address or via a well-known BGP community [17, 55].

In the other method of destination-based blackholing, the traffic will not be dropped (or re-routed) by the upstream but only flagged such that it can be dropped in the (destination) network. This can be done by performing a BGP route update to the upstream for the destination under attack which sets the next-hop to a blackhole. In IXP networks, this can be achieved by setting up a layer 2 Access Control List (ACL) on the access switches that drops all traffic destined for the MAC address of the blackhole next-hop. In order to implement this, some mechanism must exist in the IXP network to resolve the Address Resolution Protocol (ARP) queries by the CE router for the blackhole next-hop. For each of the methods, the *NO-EXPORT* BGP community can be added such that the announcement is not re-advertised to the BGP peers of the upstream.

The main disadvantage of destination-based blackholing is that good traffic headed to the blackholed destination will also be dropped. However, it does have the positive effect that the network does not get congested by the DDoS traffic. Source-based blackholing is another method of blackholing that does not share this main disadvantage of destination-based blackholing. However, it also has its drawbacks. Constantly changing spoofed IPs are often employed in DDoS attacks, which means that in practice source-based blackholing can be ineffective if there is no mechanism in place to identify spoofed IPs. Furthermore, this type of blackholing requires

additional software since it does not work out of the box with the standard BGP protocol. It can either be implemented using uRPF [6] or BGP Flowspec [35]. BGP Flowspec is an extended version of BGP that allows firewall filters to be advertised via BGP. Both methods are able to drop traffic based on source IP addresses.

Software Defined Networking
In the Software Defined Networking (SDN) paradigm, the control plane is separated from the data plane by means of a central SDN controller that issues commands to data plane forwarding devices. The SDN controller communicates via its southbound interface to the forwarding devices through a SDN protocol (e.g. OpenFlow or XMPP). Deviations from normal traffic flow behavior can be observed by the controller. Since the controller has a central position in relation to the forwarding devices, this type of setup can be used for traffic engineering and blackholing purposes. This can be done by adding and deleting flows at the SDN capable forwarding devices. If no matching flow for a packet is found in a forwarding device, the device will contact the SDN controller on how to handle the packet. This type of reactive behavior is unsuitable with respect to DDoS attacks and creates a new attack vector. The SDN controller's computational resources may be exhausted in case of an overwhelming number of queries. The overhead caused by the communication between the switches and the controller also adds additional network delay. Research has been done into these computation and communication overhead vulnerabilities, and we will discuss more about SDN in the related work section.

2.4 Related work

Remotely Triggered Blackholing (RTBH) is a technique that is applied at multiple IXPs [40, 38, 15, 16]. RTBH is used by ASes to signal their upstream via BGP that they want to blackhole a certain prefix. This technique uses BGP Community tags to signal to the route server (and thereby the connected peers) that traffic should be dropped. This way, the blackhole announcement does not need to be done to each peer individually. Dietzel et al. reveal that blackholing is frequently used and that mainly /32 prefixes are announced [16]. Also, less specific prefixes are announced for RTBH purposes by ASes connected to IXPs.

Steinberger et al. created a framework that is able to create fingerprints of DDoS traffic while keeping privacy in mind by removing the destination address [54]. The fingerprints are stored in a database called 'DDoSDB' to share real attack data and allow collaborators to query, compare and download attacks. Using the information of attacks stored in the DDoSDB, collaborators can compare attacks to improve detection and mitigation approaches. Furthermore, the researchers created STORM, a framework that is able to test and analyze a network by performing controlled DDoS attacks. A communication process is proposed by the authors "that facilitates the exchange of threat information among trusted partners and thus supports a collaborative DDoS defense".

Mirkovic and Reiher performed research into creating a taxonomy of DDoS attacks and DDoS defense methods [37]. This research looks into the way DDoS attacks are performed and allocates them into multiple classes. The authors investigate into source address validity, attack rate dynamics and the corresponding impact on the victim. Furthermore, the researchers explain the challenges that come with DDoS defense and classify the different types of DDoS defense mechanisms in existence today.

The field of artificial intelligence has multiple paradigms and methods that are useful in detecting DDoS attacks. Machine learning classification methods can be used to make a distinction between good and bad traffic. The detection tool proposed by Hsieh and Chan uses neural networks and is able to detect DDoS attacks by finding anomalies in features such as the number of packets, number of bytes, time interval variance, packet rate and bit rate [29]. Multiple appliances have been developed that are able to detect DDoS attacks based on different approaches such as Naive Bayes and Random forest trees [60]. Berral et al. implement machine learning methods to share data between network nodes [7]. The shared information is collected at a classifier, that predicts how to apply mitigation steps in case of an attack. This allows the network to detect attacks and filter them close to the source.

Fayaz et al. use an interesting approach to DDoS defense, by focusing on flexibility and elasticity in their DDoS defense system [21]. The researchers use the SDN and NFV (Network Functions Virtualization) paradigms in their DDoS defense system (called 'Bohatei'). This increases the scalability of the system since VMs are spun up using NFV depending on the size of the attack. SDN is used to route traffic through these VMs that perform scrubbing on the traffic. The authors address SDN issues that arise in DDoS attacks by proactively installing forwarding rules. Their proposed system has shown to be capable of handling attacks of 500 Gbps.

Chiesa et al. investigate into the potential of IXP environments to implement SDN methods [12]. The researchers explain the limitations of BGP and the fact that IXPs are a good place to start with innovative technologies [9]. Furthermore, they discuss that Software-Defined eXchanges (SDXes) can overcome the limitations of RTBH in DDoS mitigation [22, 27]. Namely, SDX DDoS defense methods come with more fine-grained drop policies and a higher degree programmability. The researchers mention that IXPs could provide an API to its peers, such that they can define their own drop rules.

3 Development Constraints

Our aim is to design an on-demand solution that is executed in active cooperation with the administrator of the peer AS experiencing a DDoS attack. We look into performing this process in an automated fashion, in which the customer is able to approve each important step of the process. Both the start of the detection phase and the start of the mitigation phase are initiated by the customer, such that there is no continuous active DDoS monitoring on the IXP side. This ultimately allows the customer to decide whether or not to apply the actual mitigation steps and therefore the IXP cannot be held accountable for any negative effects of the DDoS mitigation.

3.1 Design restrictions

In the IXP environment, we are subject to a number of restrictions that we have to take into account when designing the DDoS defense mechanism. The amount of traffic on the IXP network reaches peak rates of 5,6 Tbps; therefore, it is unrealistic to set up port mirroring on the switches. Analyzing this kind of data volumes is not realistic because of hardware and processing power constraints. Because of the high data rates, IXP environments often employ some type of packet sampling. In the AMS-IX network, this is done by setting up sFlow on the access switches which sends samples to a central statistics collector. AMS-IX does not include the application layer in their sFlow sampler because of ethical considerations. They only capture the link layer, network layer and transport layer. This restricts us in the sense that detecting application attacks becomes unfeasible. For our DDoS defense design, we use the AMS-IX perspective and restrict ourselves to traffic monitoring that excludes the application layer.

3.2 Defense principles

Based on the design restrictions, we determined a ranked list of several defense principles. The higher up the principle is in the list, the more valuable we consider it. These principles indicate the elements that the optimal solution should incorporate in order to be most applicable and effective in the IXP environment.

The first defense principle (P1) states that we want to be able to identify and mitigate DDoS traffic by using infrastructure and servers inside the IXP network. Since the IXP should remain neutral, we define P2 such that we give high precedence to mitigation on layer 2. This also relates to P3, where we want to emphasize that we should be conservative with respect to source-based blackholing. We want to be able to detect the most common DDoS attacks currently observed in the wild (P5). As explained, there are restrictions with respect to application layer headers. In the traffic filtering process, it is important that if traffic is dropped, the impact on good traffic is minimal (P4). In the optimal case, the traffic filtering is done before it enters the IXP network; this is outlined in P6. If this is not possible, traffic can be dropped on the PE routers without congesting the core of the IXP (P10).

The IXP network exchanges a lot of traffic, therefore the scalability of the defense mechanism needs to be considered (P7). The time needed for mitigation has to be considered as well (P8). Since DDoS attacks can have a negative impact on the victim systems, it is important that they are alleviated as soon as possible. The less configuration is required on the side of the peers, the better (P9). If there are complex configurations to be made on the CE routers, the DDoS mitigation is unlikely to become effective, since it would require all customers to implement such configurations. In the last defense principle (P11), we state that it would be advantageous if the solution makes use of existing elements in the IXP network, such that its implementation does not require the whole infrastructure to be renewed.

1. The DDoS defense intelligence resides in the IXP.
2. Identification and mitigation on lower layers is preferred.
3. The IXP must remain neutral.
4. Impact on good traffic must be minimal.
5. Detect the most prevalent DDoS attacks.
6. Drop/filter traffic as close to the source as possible.
7. Scalability of the mechanism.
8. Time need for identification and mitigation as short as possible.
9. Ideally there is no configuration required on the customer routers.
10. No congestion in the IXP core.
11. Compatibility with existing IXP infrastructure.

In the next chapter, we explain the design for the DDoS defense mechanism that we developed. This design takes into account the design restrictions and the defense principles outlined above.

4 Two-way Mitigation Design

In the next section, we explain the decisions that inspired the design. After that, we introduce the workflow of the defense process and the elements that we added to the topology of the IXP. We explain each phase of the process in detail, by means of a separate workflow per phase.

4.1 Identification and mitigation decisions

According to the Nationale Beheersorganisatie Internet Providers (NBIP) DDoS Data Report of 2017, the most common DDoS attacks in the Netherlands are amplification attacks and TCP protocol attacks (see figure 2). The NBIP DDoS Data Report predicts that the DNS amplification DDoS attack will continue to be the most popular type of attack. According to NBIP, the size of most attacks is between 1 and 10 Gbps. Amplification attacks generate a large amount of data, whereas protocol attacks consist of a large number of small packets. These types of attacks can be detected on a coarse-grained level by analyzing the bits per second (BPS) and the packets per second (PPS), respectively. Therefore, we aim to detect these two main classes of attacks using BPS and PPS as identification metrics. We perform a comparison of current traffic rates and thresholds based on historical traffic rates for these two metrics, thereby determining whether or not a destination prefix is under attack. As mentioned in section 2.3.1, we found it unreliable to identify attacks based on layer 2 alone.

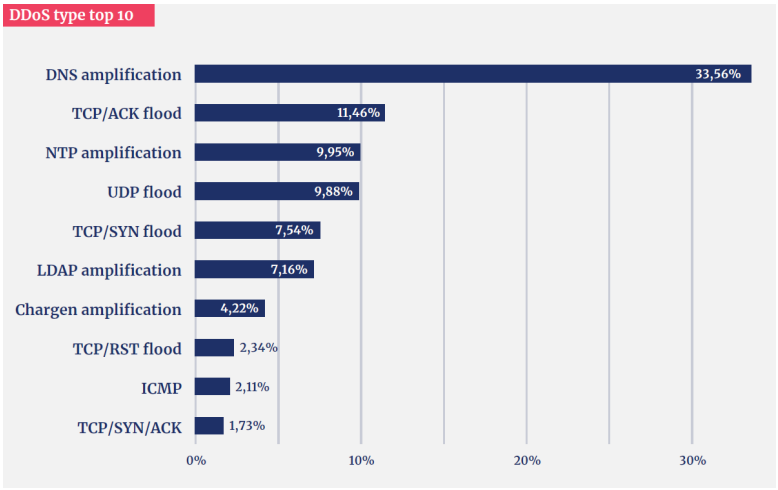

Figure 2: NBIP DDoS data report 2017 - DDoS type top 10 [44]

We find that there is potential in the IXP environment for efficient DDoS mitigation using BGP blackholing since the IXP can act from a central location by announcing the prefixes via the route server. Especially if the IXP also takes an active role in identifying the DDoS traffic, such a setup could be very effective. Another advantage is that the necessary infrastructure (the route server) is already in place at most IXPs [16, 47].

Source-based blackholing is tricky to implement in the IXP environment since false positives of source IPs in the identification process could lead to the IXP blocking traffic to and from innocent IPs in other ASes. Besides that, there is also the issue of spoofed source IP addresses that change constantly. With respect to these observations, we feel that it brings too many risks for the IXP to perform mitigation based on source IPs. Besides this, source-based blackholing (via BGP) also requires additional software and configuration on the CE routers in order to work (BGP FlowSpec or uPRF). This is yet another reason this type of mitigation is not preferable in an IXP environment in our opinion.

Therefore, we use destination-based blackholing as our main mitigation method. In this setup, the peer ASes are only allowed to approve destination prefixes to be blackholed that belong to their own network. This adheres to the defense principle that the IXP must remain neutral. A disadvantage of destination-based blackholing is that good traffic to the blackholed destination is also dropped. We find that there is a middle-ground when using destination-based blackholing; it is possible to limit the blackhole prefix announcements towards the ASes where the DDoS traffic originates from (the source ASes). This way, ASes not involved in the DDoS attack are still allowed to reach the destination prefix. We found that the most promising method of BGP blackholing in the IXP environment is the blackhole next-hop method. This allows for the IXP to absorb the DDoS traffic, and we can monitor the traffic on the ingress switch(es) to see whether or not the DDoS is still in effect.

Performing a BGP route withdrawal for the prefix under attack to the source AS has the advantage that the traffic is dropped on the CE (closer to the source). However, we found that it has several disadvantages not observed in the blackhole next-hop method. In order to check whether or not the DDoS is still active, we have to re-announce the prefix since we cannot tell whether or not the DDoS has stopped or if our mitigation

is working, because the traffic is dropped at the CE. When there is a large BGP convergence time for the route withdrawal (and re-announcement), this will prove to be a cumbersome process. Furthermore, carrying out a route withdrawal does not mean the DDoS is effectively mitigated; since it may find a different route to the destination via the transit networks of the source ASes. This could also mean that the traffic will potentially re-enter AMS-IX via another AS, which complicates the identification and mitigation process. If the traffic enters via the transit of the victim network, there are additional costs involved for the victim which is another disadvantage. We find that the only real advantage of the route withdrawal method over the blackhole next-hop method is that the peering link from the source ASes towards the IXP does not get congested. Therefore, it might be used as an optional method in case this is the issue.

Mitigation via BGP announcements is not applicable in case a source AS has not peered with the IXP's route server. This method could also fail due to the CE router of a source AS not accepting the announcement. Furthermore, the convergence time of BGP updates can be long for large networks, in which case we may decide to forfeit [52]. In these cases, we use an alternative mitigation method in which we apply a layer 2 ACL on the ingress access switches of the specific source ASes. This ACL is based upon the MAC address of the source CE router and the destination MAC address of the victim CE router. This mitigation method is more rigorous since it drops more good traffic (not just towards the destination prefix). Therefore, we prefer the blackhole next-hop method, which is the reason it is attempted first in the mitigation process.

Another consideration is to use a layer 3 ACL, which is less rigorous and can be applied to the destination prefix only. However, it is debatable whether or not this is an acceptable method since an IXP is traditionally only considered with inspecting layer 2 headers to forward (or drop) packets. One could argue the neutrality aspect of the IXP becomes endangered when layer 3 ACLs are applied to the access switches, which is the reason we have chosen to use a layer 2 ACL in our design. Note that effectively the results of the layer 3 ACL are the same as in the blackhole next-hop method. Only through using the blackhole next-hop trick we are able to drop traffic based on MAC addresses.

4.2 Design workflow

In our study to design a defense service for DDoS attacks in IXP networks, we investigated the existing techniques of DDoS identification and mitigation. We have chosen to use threshold-based detection and two separate mitigation methods in our defense mechanism. Threshold-based detection is applied since we have access to historical traffic data. This allows us to calculate thresholds to detect volumetric attacks and protocol attacks to destination IPs based on BPS/PPS metrics. We use two mitigation methods since one method is more promising than the other, but may not always be implementable. The second method is used as a backup method for the first method. We have split up the design in four separate phases. Please see figure 3 for a depiction of these four phases and how they interact. In *phase 1.1*, the prefix under attack in the victim AS is identified. In *phase 1.2*, the source ASes of the DDoS are identified and for each of these ASes a decision is made about which type of mitigation is applicable. If the mitigation in *phase 2.1* is unsuccessful or if the source AS of the DDoS attack is not peered with the route server, then the mitigation method of *phase 2.2* is applied. For traffic monitoring purposes, we use a packet sampling engine that runs on the access switches. These switches forward their traffic data to a central statistics collector. This can be done via sFlow (which is used by AMS-IX) and NetFlow. The central statistics collector is queried by our anti-DDoS component. An API is required on the statistics collector, which answers to the queries by sending the traffic data that is requested (e.g. in JSON format). We further debate this interaction and setup in the discussion (section 6).

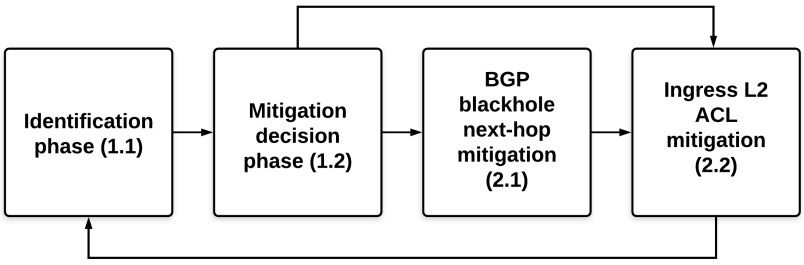

Figure 3: Four phases of two-way mitigation

4.3 Architecture

To implement the identification and mitigation approaches explained in the previous section, we add two components to the IXP infrastructure. See figure 4 for the adapted network topology including the added components. Firstly, we add a blackhole next-hop device, which is able to respond to the ARP queries of the CE routers once the BGP blackhole update is in place. Secondly, we add a DDoS Threat Mitigator (DTM) device, which contains the intelligence for identifying and mitigating attacks.

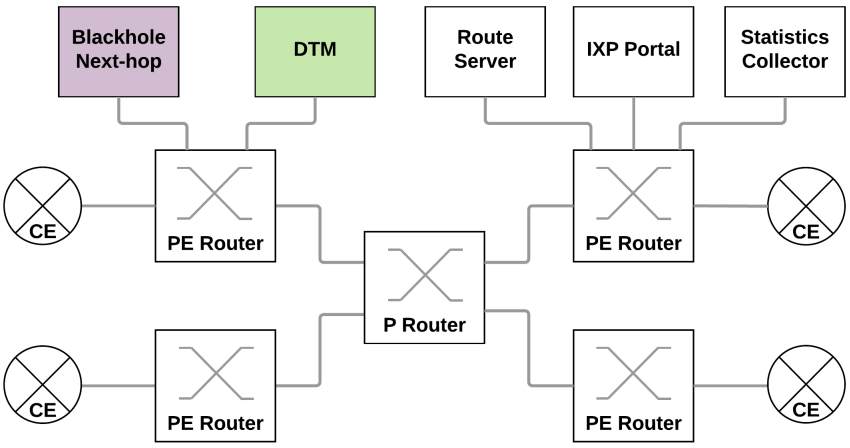

Figure 4: Abstract network topology

See figure 5 for the interaction between the components used in our defense mechanism. The DTM is the central component of the architecture that communicates with all other components. It issues orders to the route server and PE routers to implement the two mitigation methods used. It also interacts with the IXP portal, which requires additional functionality for the customer to initiate the defense mechanism, and also for the DTM to request information used in the identification and mitigation phases (phase 1.1 and phase 1.2). The DTM queries the statistics collector to obtain information about the monitored traffic. This is mainly done by means of two sub-elements, namely the DDoS Threshold Adviser (DTA) and the Current Traffic Analyzer (CTA). These elements perform traffic data calculations for destination prefixes in the peer ASes. On the IXP network, the amount of traffic that traverses the network is so large that it is unrealistic to monitor all traffic. This makes port mirroring unsuitable. In the AMS-IX network, the sampling rate is 1 in every 1600 packets. See figure 6 and figure 7 for the functionality of the DTA and CTA, respectively.

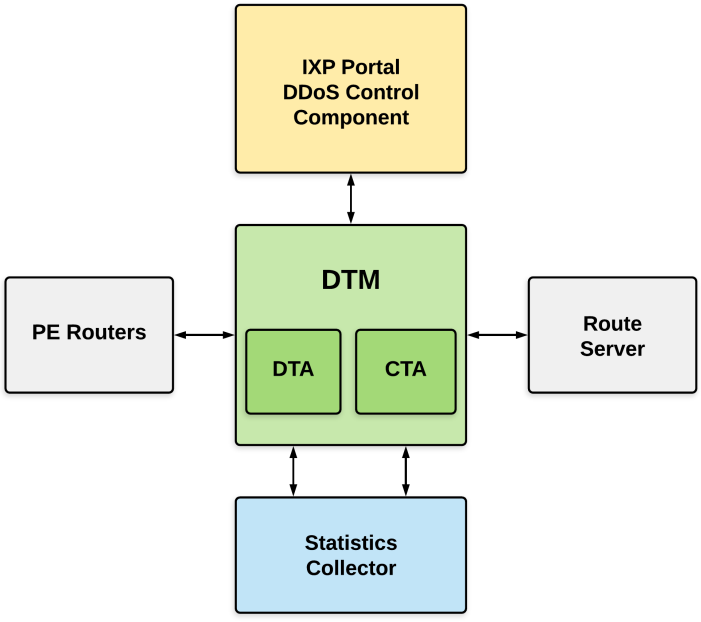

Figure 5: Component interaction

The DTA is responsible for calculating thresholds (BPS and PPS) using historical traffic data. The DTA is used in the identification phase (1.1), where its output is used to determine which destination prefix(es) are under attack. This is done by making a comparison to the output of the CTA. The information retrieved by the DTA in the identification phase (1.1) is also used in the mitigation decision phase (1.2), to calculate thresholds for source ASes in order to determine which ASes are originating DDoS traffic. Therefore, the border line of the first action in the DTA figure is dashed, since this step is only performed once in the process. There is an exception to this in case the thresholds have to be recalculated when the DDoS attack lasts for an extended period of time. This needs to be done since the traffic rates differ per time of day. Note that this process is not reflected in the workflows of section 4.5.

Requests to the DTA are based on certain input parameters. These input parameters will specify to the DTA which phase of the mitigation process is currently active, as well as which information the DTA should query from the statistics collector. In the identification phase, the DTA will request data for the prefixes in the victim AS. We will explain how these destination prefixes are obtained in section 4.5.1 corresponding to the identification phase. These prefixes correspond to prefixes announced by the victim AS. After that, in the mitigation phase, the DTA will perform operations based only on the prefix under attack. The DTA will query data for all destination IPs in the input prefix range(s), and aggregate this data to the specific prefix(es). The input parameters also specify which source MAC addresses and destination MAC address to filter on. This way, traffic from the source ASes to the victim AS can be identified, such that the ASes that are originating DDoS traffic can be determined. All of this data is available in the sFlow version 5 protocol format [43].

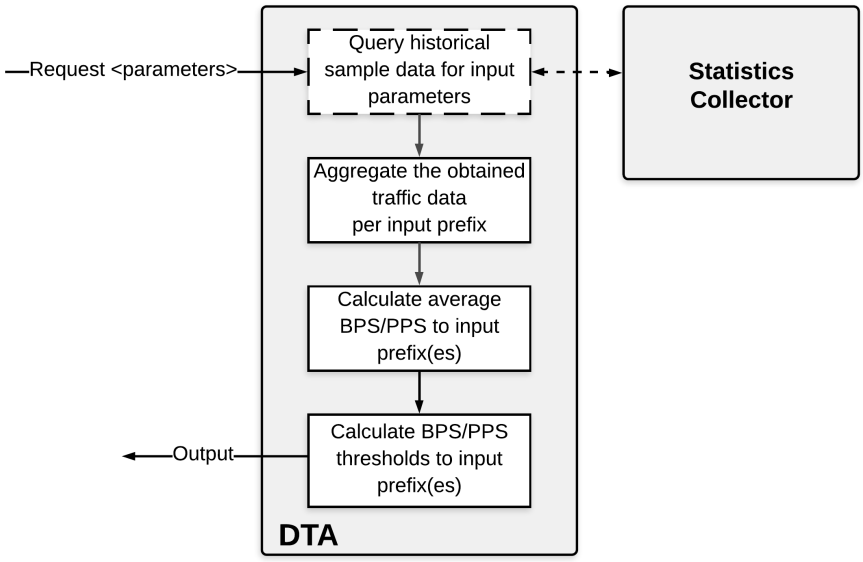

Figure 6: DTA component

The CTA is responsible for analyzing the current traffic rates (BPS and PPS). It takes as input the parameters on which to filter, which are different per phase (and mitigation method). We will discuss this further in the sections of the corresponding phases. The input parameters used in the CTA are the same as those used in the DTA in each corresponding phase since the results of these two components are compared. The CTA is used in every phase, whereas the DTA is only used in the first two phases. This is because once the thresholds are calculated, the CTA can compare its output to these earlier determined values. As explained, there is an exception to this; new thresholds need to be calculated in case the DDoS persists over a prolonged period of time (e.g. longer than 30 minutes to an hour). The exact timing is yet to be determined in future work.

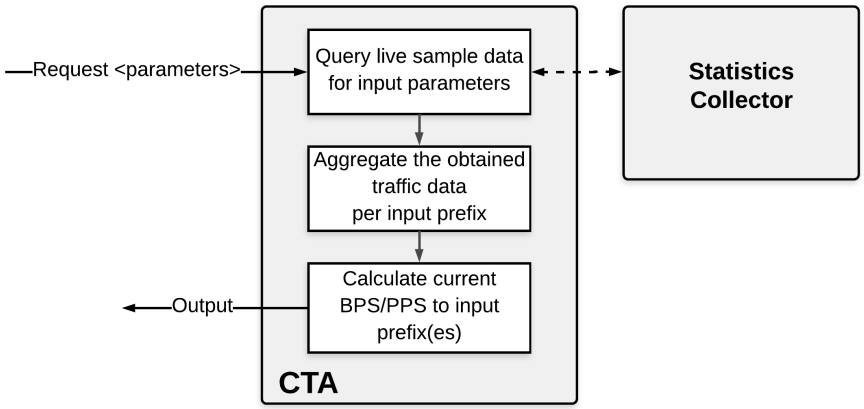

Figure 7: CTA component

4.4 Mitigation overview

In figure 8 we show an example topology where AS I and II are originating DDoS attack traffic to AS III. AS I is peered with the route server whereas AS II is not peered with the router server. In the case of AS I, mitigation via BGP announcement is performed. In the case of AS II, BGP announcements are not an option and mitigation via the more coarse-grained layer 2 ACL is applied. For both the BGP blackhole next-hop mitigation and the ingress layer 2 ACL mitigation, a layer 2 ACL is placed on the ports of the PE routers facing the core of the IXP. Thus, we do not put ACLs on customer ports without their permission and the packet capture engine is still able to monitor traffic. In case of the BGP blackhole next-hop mitigation, the layer 2 ACL drops traffic destined to the MAC address of the blackhole next-hop. In this manner, all traffic destined for the blackholed prefix is dropped on the ingress PE router. For the ingress layer 2 ACL mitigation, the ACL drops traffic based on the MAC address of the source CE router and the MAC address of the victim CE router. The victim AS is still able to receive traffic from the other ASes that are not part of the DDoS attack (AS IV).

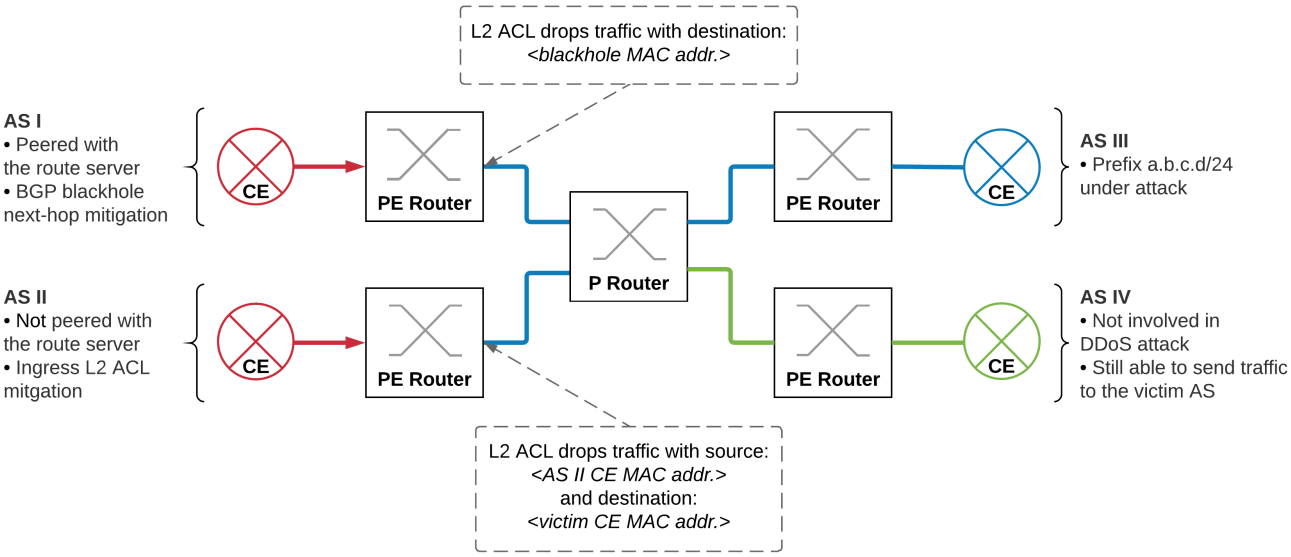

Figure 8: Simplified IXP topology including a DDoS attack

4.5 Phase workflows

4.5.1 Identification phase

The main purpose of the identification phase is to identify the prefix(es) in the victim AS that are under attack. See figure 9 for the workflow of this phase. The administrator of the victim AS initiates the DDoS defense mechanism on the IXP portal. At that point the identification process starts. Also, the administrator can decide which prefixes to mitigate once the identification process is successful. These two actions are shown in

turquoise color on the workflow. The phases that follow are set up using the destination prefix the administrator selected as the prefix to perform mitigation upon.

The identification process is as follows. Firstly, the IP and MAC address of the victim's CE router are looked up to filter the traffic based on that. Furthermore, the IXP portal is checked to determine whether or not the victim's CE router is peered with the IXP's route server (RS). If this is the case, we are able to query to the route server to obtain destination prefixes advertised by the victim AS. If not, we generate these prefixes on the fly by aggregating IPs that we observe in current traffic. We focus on calculating thresholds for /24 destination prefixes rather than more specific prefixes. This is mainly because of scalability reasons since it is computationally expensive to calculate and store thresholds for each individual destination IP.

The DTA and CTA now query the statistics collector for historical traffic and current traffic destined for the MAC address of the victim's CE. For each of the earlier determined destination prefixes, the DTA calculates thresholds based on BPS and PPS. The CTA calculates the current BPS and PPS for the destination prefixes. After comparing the results of the DTA and the CTA, the administrator of the victim AS is presented on the IXP portal with the prefix(es) for which the BPS and/or PPS threshold is exceeded. At that point, the administrator can decide to start the mitigation phase (per destination prefix). We will refer to the destination prefix that is chosen to mitigate as the 'mitigation prefix' from now on.

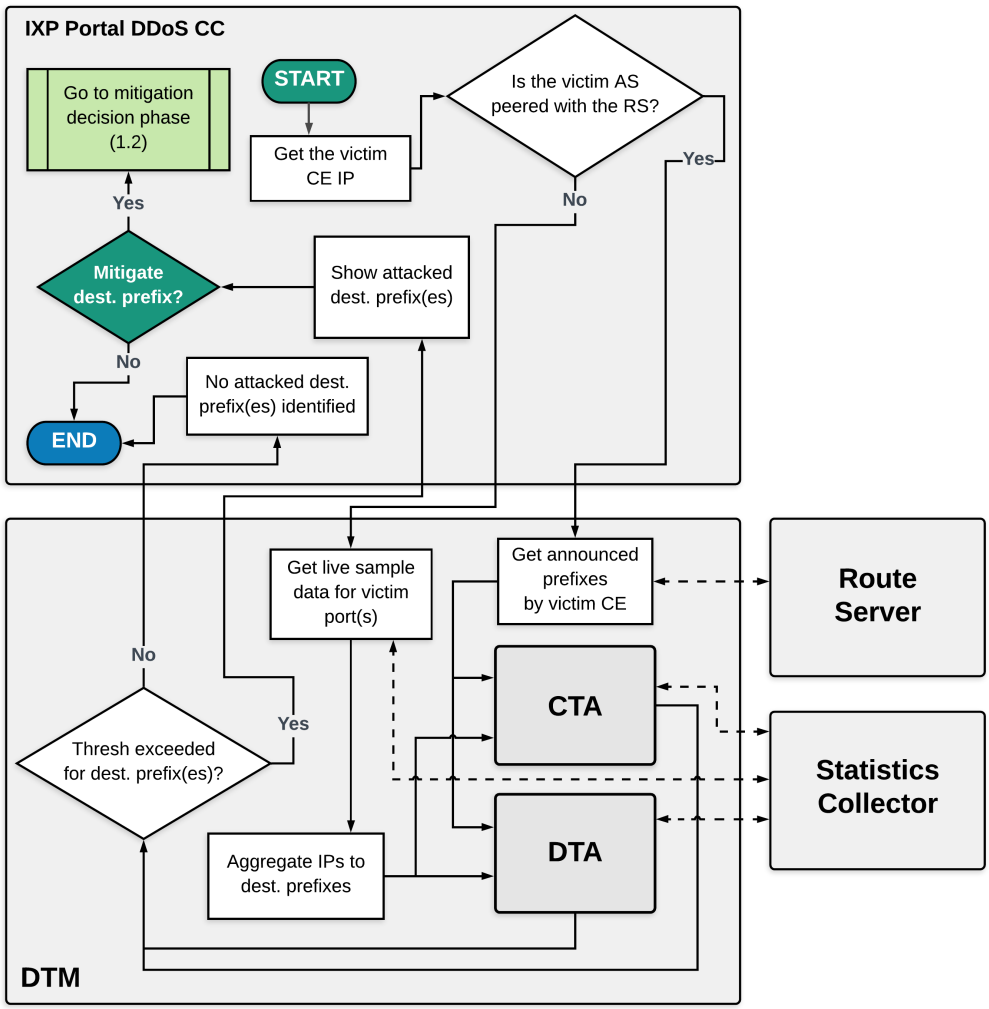

Figure 9: Workflow of identification phase (1.1)

4.5.2 Mitigation decision phase

The primary goal of the mitigation decision phase is to decide which ASes are originating DDoS traffic, and consequently to determine which mitigation method to apply for each of these source ASes. The process forks after this point since different mitigation decisions can be made for the involved source ASes. See figure 10 for the workflow of this phase. The entry-point of this phase through the previous phase is indicated by the *START* action. In case of a VPS setup used in an attack, it is possible that the DDoS originates from a single AS; if a VPS cluster is hosted by a single provider these servers could reside in the same AS. However, generally

speaking, DDoS attacks originate from all over the Internet (multiple ASes).

Firstly, the MAC addresses of the CE routers relating to the source ASes need to determined. The CTA will now be executed again, and it will request traffic which is destined for the mitigation prefix (and the MAC address of the victim's CE router). The CTA will determine which ASes are currently sending the highest amount of traffic (BPS/PPS) to the mitigation prefix. This is done for scalability reasons, such that not all ASes need to be investigated. The ASes can be identified by the MAC address(es) of their CE router(s). The ASes that have a high amount of traffic towards the victim AS are further investigated in the next step by the DTA. The DTA will calculate thresholds for these ASes. The thresholds are based upon the BPS/PPS of the source ASes towards the mitigation prefix. The data that was obtained in the previous phase by the DTA is used here (since this also contained data for the mitigation prefix). The output of the DTA and CTA is compared to determine the source ASes that have a higher BPS/PPS than usual.

Once the source AS(es) are identified, for each of them the mitigation method is determined. The blackhole next-hop method is preferred; however, this is only possible if a source AS is peered with our route server. If this is not the case, we cannot send BGP announcements towards the AS. If the source AS is not peered, we enter the ingress layer 2 (L2) ACL mitigation phase.

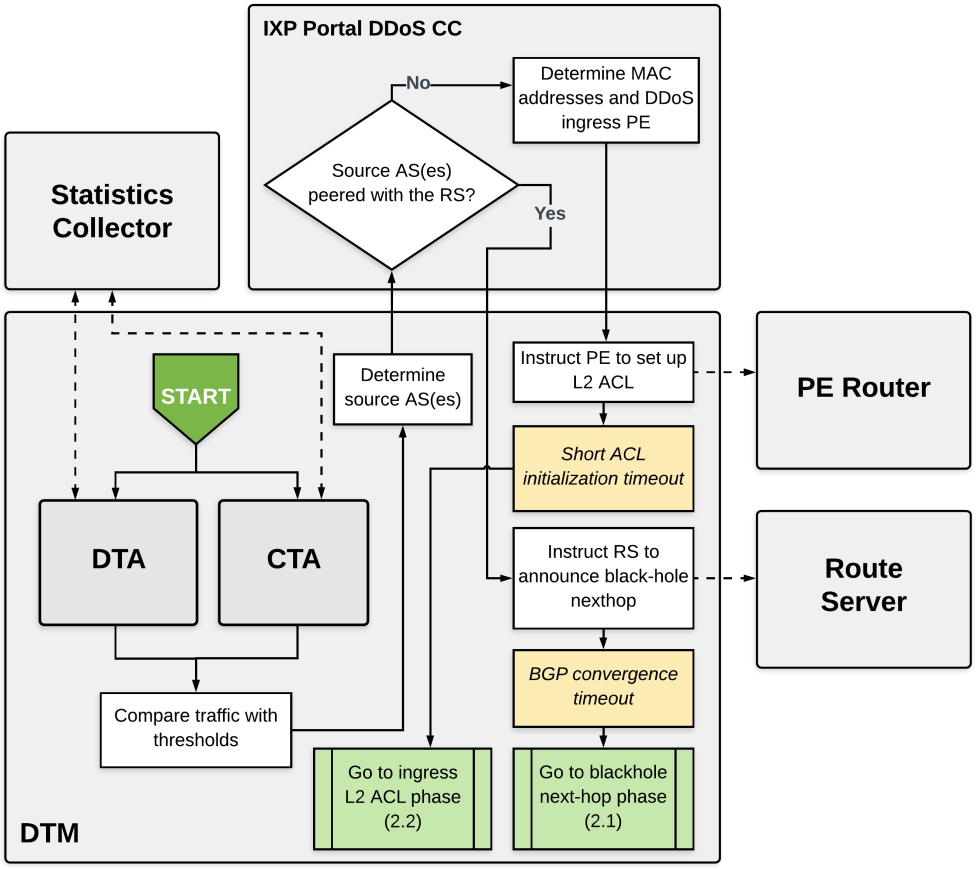

Figure 10: Workflow of mitigation decision phase (1.2)

4.5.3 Blackhole next-hop mitigation phase

The blackhole next-hop phase starts after the BGP convergence timeout in the previous phase. See figure 11 for the workflow of this phase. The BGP convergence timeout is dynamically determined and may differ per source AS. This is because larger networks may have larger BGP convergence times [52]. When the convergence timeout is finished, the CTA requests new traffic data to analyze and calculate the traffic metrics for each source AS. This is done by querying the statistics collector for data where the source MAC addresses match those of the CE routers of the source ASes, and the destination matches IPs in the mitigation prefix. The output is compared to the earlier determined thresholds per source AS in order to decide whether or not the mitigation is successful.

In case the current BPS/PPS has dropped below the threshold, we conclude that the mitigation is successful for that specific source AS and keep the BGP blackhole next-hop method in place until the DDoS attack subsides. This is done by means of a timeout loop, in which we wait for a certain period of time before we perform the threshold comparison again with new traffic data. The shorter this timeout, the more the statistics

collector is queried for new data and the quicker there is feedback about whether or not the DDoS attack is still in effect. The thresholds used were calculated earlier in phase 1.2. Please note that if the DDoS persists for an extended period of time, new thresholds need to be calculated since they may not be sufficiently fine-grained with respect to the time of day. This is not shown in the workflow figure.

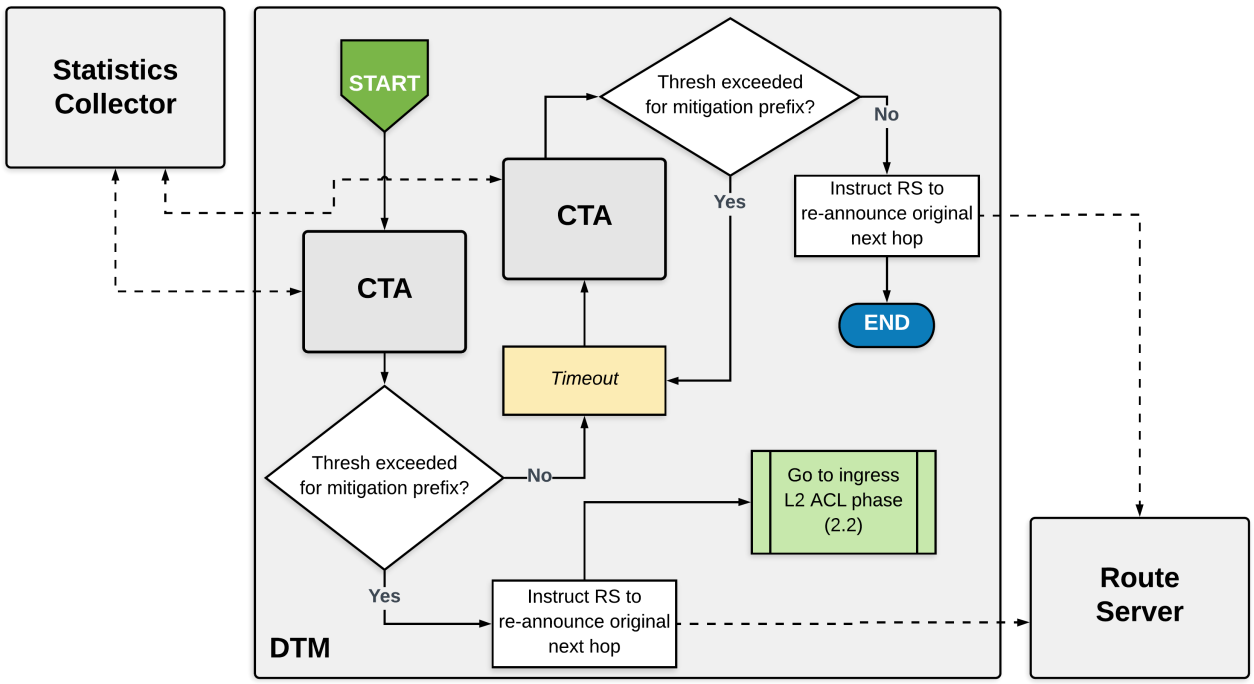

Figure 11: Workflow of blackhole next-hop mitigation phase (2.1)

4.5.4 Ingress layer 2 ACL mitigation phase

This phase uses a SDN approach to mitigate the DDoS traffic. If a source AS is not peered with the route server, this technique is used instead of mitigation via BGP announcements. It is more coarse-grained than the mitigation approach used in the previous phase and therefore used as a last resort. Note that the ACL initialization timeout of phase 1.2 is very short, since this mitigation method should be in effect almost instantly. See figure 12 for the workflow of this phase. In the case that the BGP mitigation approach was unsuccessful, the ACL still needs to be put in place. After that, a timeout loop similar to phase 2.1 is used until the DDoS traffic has ceased to enter the network. The CTA operations and threshold comparisons are performed in a similar fashion to the previous phase. In case the victim AS still experiences issues, the identification process is re-started since the mitigation methods were unsuccessful.

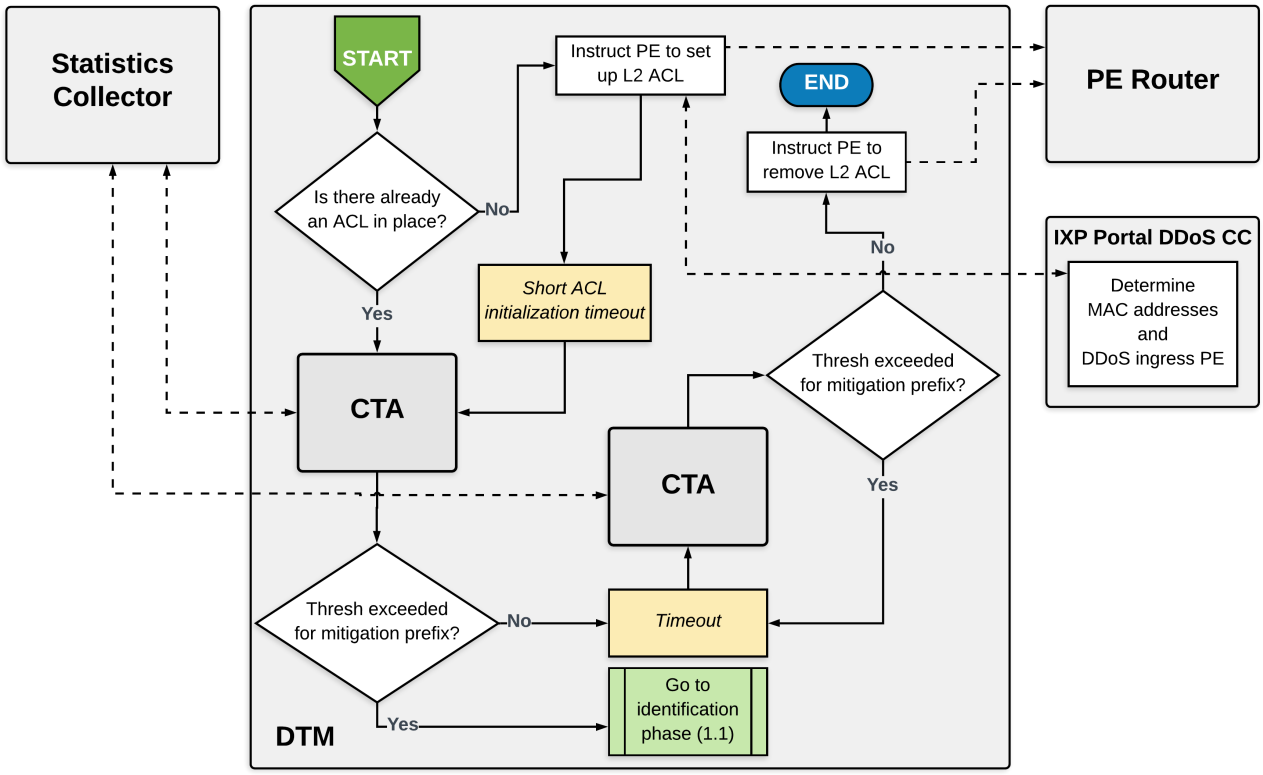

Figure 12: Workflow of layer 2 ACL mitigation phase (2.2)

5 Experimentation

In order to test the interaction between the components as outlined in section 4, we set up an experiment that simulates the design. This experiment focuses on the two mitigation phases (2.1 and 2.2) as it does not include the identification phase. The proof of concept (PoC) shows how our proposed design responds when the BPS threshold is exceeded. Both the BGP blackhole next-hop method and the ingress L2 ACL mitigation method that we propose in our design, are implemented in this PoC.

The IXP environment is simulated with two ASes connected to it. AS I functions as the source AS and AS III functions as the victim AS. Normal traffic to AS III is sent via the OpenvSwitch bridge to simulate other peers connected to the IXP network. The DDoS attack is simulated from AS I to AS III. The PoC does not include the identification phase. At the start of the experiment, the source AS is already identified, and the thresholds are set. The victim network of AS III is actively monitored by the DTM. Whenever the threshold exceeds, the system will start the mitigation process as described in our proposed two-way mitigation design.

5.1 Experimental setup

The setup of the experiment consists of multiple components, namely the DTM (FastNetMon), a route server, two CE border routers, OpenvSwitch and the endpoints. For the experiment we used three identical Dell PowerEdge R210 servers. The specifications of those servers are described in Table 1. The DTM, route server, blackhole next-hop, and endpoints run as virtual machines (VMs). Each VM runs the same version of the Ubuntu 16.0.4.4 LTS as operating system. An overview of all components can be seen in figure 13. The setup we use in this experiment has some limitations in the amount of traffic that we can generate. This is most likely due to the VirtualBox VM setup of the endpoints. Therefore, the volume of traffic we generate is not similar to the traffic traversing an IXP. The primary goal of this PoC is to clarify the interaction that takes place between the different components to achieve the mitigation approaches.

CPU	Intel(R) Xeon(R) CPU L3426 @1.87GHz
RAM	Micron DIMM DDR3 Synchronous 1066 MHz 8GB
Network card	Broadcom NetXtreme II BCM5716 Gigabit Ethernet (1Gbit/s)
Operating system	Ubuntu 16.04.4 LTS
Hypervisor	Oracle VM VirtualBox Manager 5.1.34_Ubuntu

Table 1: Specification of Dell PowerEdge R210

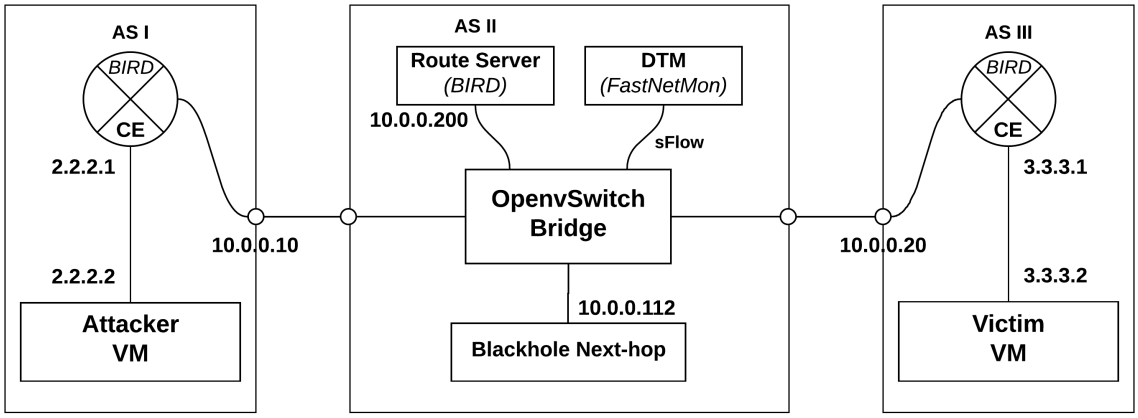

Figure 13: Experimental setup

CE routers
Each CE runs on a separate Dell PowerEdge R210 server and uses BIRD to peer with the route server. This enables AS I and AS III to learn the advertised prefixes and allows them to reach each other via the OVS bridge. In this setup, the DDoS traffic originates from AS I and AS III is the victim.

Endpoints
Within both of the peer ASes an endpoint is simulated. Both endpoints set their default gateway to the CE router of their corresponding AS. For our setup, generating traffic with iPerf is acceptable since we are concerned with triggering a bandwidth threshold to simulate a volumetric attack [32]. The attacker VM in AS I generates 150 Mbps of traffic to the victim VM in AS III.

IXP network
The OpenvSwitch (OVS) bridge represents the IXP environment. OVS is a virtual switch that is well suited to function as a virtual switch in VM environments [24]. In this experiment two CE routers are connected to the OVS bridge. The OVS bridge provides the DTM with sFlow data with a polling interval of 10 seconds and a sampling rate of 1/64 packets. In order to simulate regular traffic to AS III, iPerf is used to generate network traffic with a traffic rate of 50 Mbps.

DTM
The DTM is implemented using FastNetmon [20]. FastNetMon is an open-source threshold-based DDoS analyzer tool that can be used with multiple packet capture engines. This tool can be seen as the DTM component of our design (excluding the DTA). The DTM receives the sFlow data from the OVS bridge and keeps track of the BPS and PPS from AS I to the mitigation prefix. Since the DTA is not part of our experiment, we set the threshold manually to 150 Mbps. Whenever the threshold is exceeded, FastNetMon generates an alert that the mitigation prefix is under attack. We pipe this alert to our mitigation script (written in Python) that executes the mitigation process. The mitigation script checks if the source AS is connected to the route server. If this is the case, the DTM applies filters on the route server which announce the blackhole IP address to AS I as the next-hop to reach the mitigation prefix. Furthermore, the script is able to instruct OVS to apply layer 2 ACLs. After the appliance of a mitigation method, the DTM in our PoC checks if the threshold is still exceeded to conclude if the mitigation is successful.

Route server
The route server runs BIRD [8] to advertise routes from AS I to AS III and vice versa. BIRD is configured such that it functions as a route server and does not add itself as a next-hop. The mitigation script that is executed

on the DTM applies filters to routes per AS and reconfigures BIRD to update these filters. An example of changing the next-hop of the *3.3.3.0/24* prefix to the blackhole next-hop address is shown in listing 1. This filter is only applied on the export of routes to the source AS of the DDoS (AS I).

```
filter traffic_next_hop { if net ~ [3.3.3.0/24] then {
    bgp_next_hop = 10.0.0.112; accept;
} else
    accept;
}
```

Listing 1: BGP blackhole next-hop mitigation in BIRD

5.2 Testing scenarios

The experiment we perform consists of three scenarios as outlined in table 2. Since our design uses a different mitigation method if the source AS is not peered with the route server, three scenarios occur. In the first scenario, the source AS is peered with the route server and the BGP blackhole next-hop mitigation succeeds. In scenario two, the source AS is also peered, but the BGP blackhole next-hop mitigation fails and the ingress layer 2 ACL is applied. If the source AS is not peered with the route server, only the ingress layer 2 ACL mitigation method can be applied, which represents the third scenario.

Scenario	Peered with RS	BGP blackhole next-hop	Ingress L2 ACL
1	✓	✓	
2	✓	✗	✓
3	✗		✓

Table 2: Mitigation scenarios in experiment

5.3 Results

In this chapter we elaborate on all the results that are gathered during the experiment. Per scenario we describe the results and afterwards make some final remarks.

5.3.1 Scenario 1

In this scenario the source AS is peered with the route server and the DTM succeeds in mitigating the DDoS attack using the BGP blackhole next-hop mitigation method. This can be observed in figure 14. The DTM notices the exceeded threshold and starts the mitigation at *t1* (25 seconds). At *t2* (35 seconds) the BGP convergence timeout is finished and at *t3* (40 seconds) the DTM concludes that the mitigation is successful.

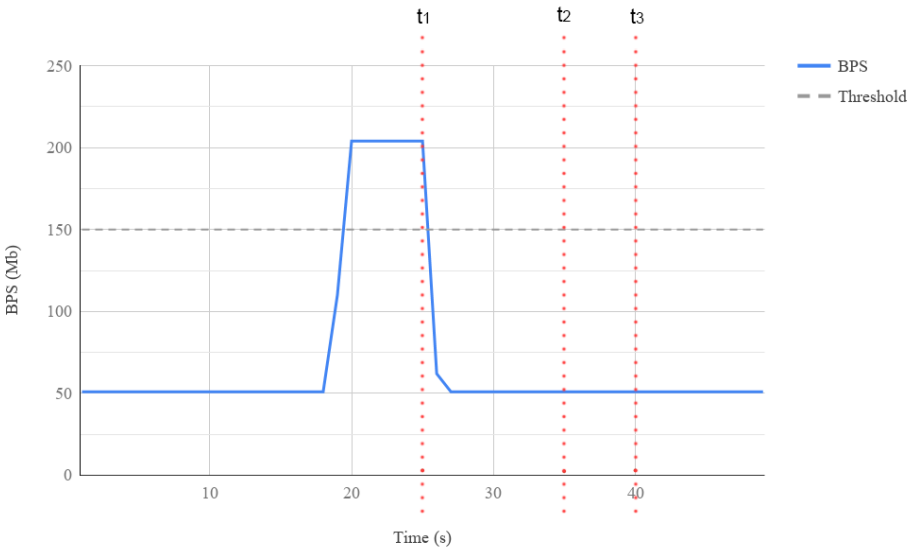

Figure 14: Mitigation scenario 1

5.3.2 Scenario 2

In this scenario the source AS is also peered with the route server. However, the BGP blackhole next-hop mitigation is unsuccessful and the DTM proceeds to use the layer 2 ACL mitigation method. As can be seen in figure 15, the DTM identifies the exceeded threshold and immediately starts the BGP blackhole next-hop mitigation at *t1* (25 seconds). At *t2* (35 seconds) the DTM finishes the BGP convergence timeout and at *t3* (40 seconds) it concludes that the BGP blackhole next-hop mitigation is unsuccessful. The DTM starts the ingress L2 ACL mitigation at *t3* and concludes that this mitigation approach is successful at *t4* (45 seconds).

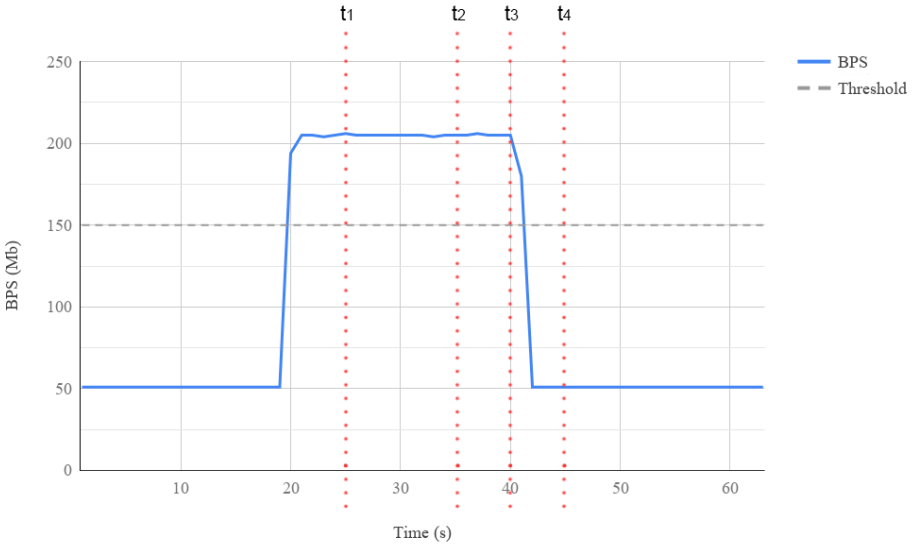

Figure 15: Mitigation scenario 2

5.3.3 Scenario 3

In this scenario the source AS is not peered with the route server. The DTM succeeds in mitigating the DDoS attack using the ingress L2 ACL mitigation method. As can be seen in figure 16, the DTM identifies the exceeded threshold and immediately starts the ingress L2 ACL mitigation at *t1* (25 seconds). At *t2* (30 seconds) the DTM concludes that the mitigation is successful since the threshold is no longer exceeded.

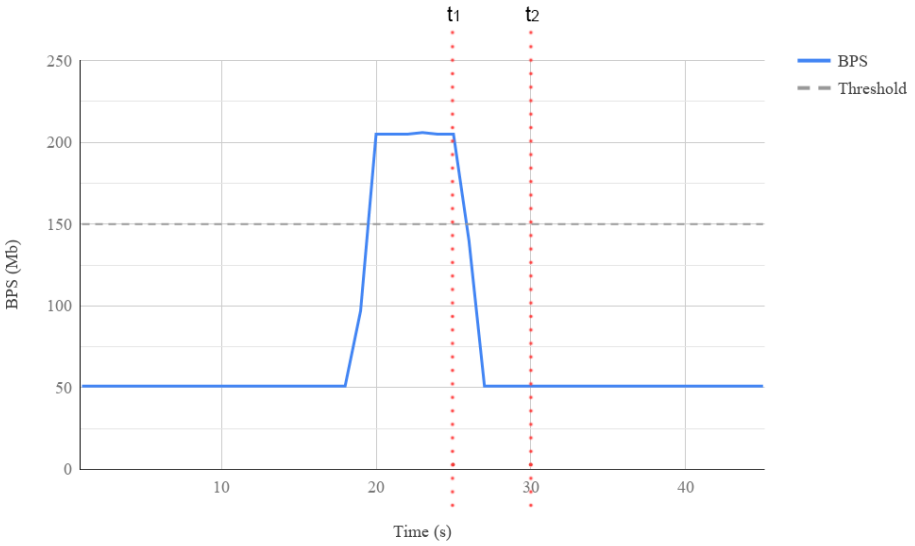

Figure 16: Mitigation scenario 3

During the experiment we observed that using BPS thresholds to perform mitigation methods was successful in each of in the three scenarios. We were able to show that this setup is able to identify a prefix exceeding the

threshold and execute the applicable mitigation technique. This is done with our two-way mitigation approach using OVS to send sFlow data to the DTM (FastNetMon).

6 Discussion

For traffic monitoring purposes, we chose to use packet sampling engines on the access switches instead of switch counters, since the counters show less information. The sample data should contain the MAC addresses and IP addresses of the traffic. This is an important requirement for the packet capture engine. Furthermore, the TCP and UDP port numbers can be used to provide the customer with additional information on the type of attack. Although we do not use pattern matching, other info such as the length of the packets would also be useful as an extension to the identification mechanism. The sampling rate within the AMS-IX network on the PE routers is set to 1 in every 1600 packets. Through extrapolation, we are able to approximate the actual traffic volumes. Since the amount of traffic in IXP networks is very high, this sample rate can still give a realistic view of the traffic. The lower the sample rate, the less accurate the extrapolation will become. Therefore, experimentation needs to be done with respect to different sample rates and the way they relate to our identification mechanism.

The thresholds for each identification metrics must be determined in a fine-grained manner. The threshold needs to be determined based on the time of day the DDoS attack occurs. Furthermore, the threshold should be calculated over a long period of time, where the most recent data is taken into account at higher weights. The threshold could, for example, be set to a certain percentage above the average traffic at that time of day. The threshold calculation mechanism needs additional testing and experimentation.

The main aspect of discussion for our proposed defense mechanism is scalability. As mentioned, the IXP network exchanges large amounts of data and many different ASes are connected. In order to identify DDoS attacks in this infrastructure, many aspects need to be taken into account. In our design, we apply threshold-based detection. The thresholds are calculated based on historical data obtained from the statistics collector. The efficiency of the process depends on multiple aspects. One part is the retrieval of the data on the side of the statistics collector that was queried by the DTM. To increase the speed of this aspect, it would be advantageous to have an indexing mechanism at the statistics collector such that the data can quickly be retrieved. This indexing should be based on MAC addresses of the CE routers and destination IP addresses, which are the main parameters used by the DTM to request information. Secondly, the speed at which the data is sent across the network towards the DTM is a factor. To speed up this process, the two machines could be connected with a dedicated pipe. Alternatively, the DTM could exist on the same box as the statistics collector. The third point of contention is the computational time at the side of the DTM to calculate the thresholds. The algorithms used for these calculation purposes should be as efficient as possible, and the machine running the DTM should have abundant computational resources to speed up this process. Practical testing with real sample data must be done to achieve more insights into the scalability of the entire process.

In the current design, we use two types of layer 2 traffic filtering. One of the types is instigated via BGP traffic engineering, whereas the other is a more coarse-grained layer 2 ACL. Obviously, BGP traffic engineering is not a layer 2 solution. However, once the BGP route update is in place on the CE routers, DDoS traffic entering the IXP network can be filtered based on layer 2 ACLs. We felt these two types of mitigation were most compatible with the IXP environment. Two other mitigation we investigated into but did not make the final design are BGP route withdrawal mitigation and layer 3 ACL mitigation. As explained earlier, we felt these mitigation methods were not compatible with our standards. However, if the IXP community would comply with applying layer 3 ACL mitigation, we do believe this is the only method that is required and that it is superior to layer 2 ACLs. In case of a layer 3 ACL, there is no need for a blackhole next-hop BGP announcement, which effectively achieves the same result on layer 2. Thus, the two-way mitigation design would not be needed in this situation. In the layer 3 ACL method, there is no dependency anymore on the source AS being peered with the route server and also no BGP convergence time, which are two advantages of this method.

The BGP convergence timeout is used in the blackhole next-hop method to wait for the BGP route update to be applied at the CE router(s) of the source AS(es). In our project, we have not developed a method to determine how this timeout should be calculated for each AS. If this timeout is exceeded, we apply the layer 2 ACL mitigation method. In certain cases, the decision could be made to skip the BGP announcement mitigation and immediately perform layer 2 ACL mitigation if immediate mitigation is required.

With scalability in mind, in the present design we identify DDoS attacks based on 'coarse-grained' prefixes. For destination-based blackholing ideally more specific prefixes should be used. This way, the impact on good traffic is minimized. As an improvement to our design, a mechanism needs to be developed that is able to identify the exact destination prefixes that are under attack. For example, once the coarse-grained prefix receiving an abnormal amount of traffic is identified, additional detection steps could be performed to identify the /32 prefixes under attack. Then these prefixes could be used in the blackhole next-hop method or optionally with layer 3 ACL mitigation. One additional consideration to be made here is that the CE routers of the source ASes will need to be configured to accept more specific prefixes. Thus, although it is advantageous to announce

more specific blackhole prefixes, in practice this may cause the method to fail in case the CE routers are not configured the right way.

7 Conclusion

In this research project, we have created a design proposal for defense against DDoS attacks in IXP environments. We base our design upon multiple defense principles and operate within a set of design restrictions that come with the IXP network. The defense process is initiated by the administrator of the victim AS that is under attack. To effectively detect DDoS attacks, we calculate thresholds based on historical data. Once the identification process is complete, the administrator decides on which prefixes to apply the mitigation mechanism.

For each AS that is identified as being involved in sending DDoS traffic to the victim, we determine the appropriate mitigation method. In our mitigation approach, we are able to drop traffic on layer 2 at the access switches. If the blackhole next-hop mitigation method is applied, destination-based filtering is executed based on the IP prefix to mitigate. This method is initiated through BGP traffic engineering. The disadvantage of this method is that it is only possible if a source AS is peered with the IXP's route server. Furthermore, BGP convergence time is to be taken into account. For the alternative layer 2 ACL mitigation method that we propose, the traffic filtering is more coarse-grained and will cause good traffic originating from the source AS to the victim AS to drop. Therefore, we prefer the blackhole next-hop method. Alternatively, the usage of a layer 3 ACL could be considered to alleviate this negative impact on good traffic.

We focused on integrating the available tools in the IXP environment into our design. We made use of the route server and access switches for mitigation purposes, and the statistics collector for identification purposes. Hence, the design is compatible with IXP environments in general and its implementation should be possible without adding many new components to the network. The scalability of the design is an important factor, which can be tested using real-life IXP traffic statistics. The components we add to the network are the DDoS Threat Mitigator (DTM) and the blackhole next-hop ARP dummy. The DTM is the central element that communicates with the other components in the network. The DDoS Threshold Adviser (DTA) and Current Traffic Analyzer (CTA) are sub-components of the DTM that are used for identification and traffic analysis purposes. An extension to the IXP portal (customer side and IXP side) is required to integrate our design. The design we propose is an on-demand service that can be requested by the customer and automates the identification and mitigation of DDoS attacks.

8 Future Work

Our study has looked into several mitigation approaches and used the most compatible as part of the defense mechanism. More research can be done into DDoS identification methods. In this study, we focused on threshold-based detection since we found it promising and were interested in how it could be applied to the IXP environment. As mentioned in the related work section, there are methods of using artificial intelligence to detect DDoS attacks. If an IXP compatible method exists that does not require historical data to detect attacks, this would be interesting since it would impact the efficiency of the design in a positive way. Using AI, if multiple ASes continuously send a high amount of data to a specific destination, how do we know which one is the perpetrator? This type of identification would require more complex identification patterns in order to detect the different types of DDoS attacks. In our research we focused on identification and mitigation on the lowest possible level. Equally sized packets and destination ports are possible metrics that could still be integrated into our design.

The design proposed in this research study is not yet fully optimized. It is the result of a theoretical analysis and proposes a defense mechanism that can be implemented in an IXP infrastructure. The design requires additional practical testing in order to increase the efficiency and effectiveness. This is the main area of future research. For example, testing needs to be done with different sample rates of the packet capture engine. By doing this, one could examine if extrapolated sampled traffic resembles real traffic to the right degree in order to perform our identification methods. Another interesting aspect for future research is to determine how quickly an attack can be identified in real IXP environments and what the total mitigation time is. The main question to be answered here is if the design indeed scales to IXP infrastructures. This depends largely on the specification of the statistics collector and the DTM as well as on the efficiency of the algorithms used.

Another area to further this research is to define different types of mitigation per type of DDoS attack. In our current approach, we strive to detect volumetric (e.g. UDP amplification) and TCP protocol attacks based on BPS and PPS metrics. However, we treat both classes of attacks the same when it comes to mitigation. Using a different mitigation approach for the protocol attacks and other types of attacks could be considered. The NaWas is an available option here since the AMS-IX network connects directly to it. This would involve automatic redirection to the NaWas for identified attacks, and re-routing to the customer network once the

traffic is scrubbed. Additional detection metrics on layer 4 in our threshold-based detection as well as pattern matching would be beneficial to detect more advanced DDoS attacks.

9 Acknowledgements

We would like to show our gratitude to our supervisor Stavros Konstantaras from AMS-IX for his guidance and expertise during this research project. This accomplishment would not have been possible without him. Furthermore, we are thankful to the reviewers for sharing valuable comments on this research.

References

[1] Kanak B Agarwal, John B Carter, Colin K Dixon, and Jeffrey T Rasley. Port mirroring for sampling measurement of network flows, December 1 2015. US Patent 9,203,711.

[2] Bernhard Ager, Nikolaos Chatzis, Anja Feldmann, Nadi Sarrar, Steve Uhlig, and Walter Willinger. Anatomy of a large European IXP. *ACM SIGCOMM Computer Communication Review*, 42(4):163–174, 2012.

[3] AMS-IX. Amsterdam Internet Exchange AMS-IX Infrastructure, . Available at `https://ams-ix.net/technical/ams-ix-infrastructure` (Accessed on 03/07/2018).

[4] AMS-IX. Amsterdam Internet Exchange Statistics, . Available at `https://ams-ix.net/technical/statistics` (Accessed on 03/07/2018).

[5] AMS-IX. Amsterdam Internet Exchange Trusted Networks Initiative, . Available at `https://ams-ix.net/technical/trusted-networks-initiative` (Accessed on 22/06/2018).

[6] F. Baker and P. Savola. Ingress Filtering for Multihomed Networks. BCP 84, IETF, March 2004.

[7] Josep L Berral, Nicolas Poggi, Javier Alonso, Ricard Gavalda, Jordi Torres, and Manish Parashar. Adaptive distributed mechanism against flooding network attacks based on machine learning. In *Proceedings of the 1st ACM workshop on Workshop on AISec*, pages 43–50. ACM, 2008.

[8] BIRD. The BIRD Internet Routing Daemon Project. Available at `http://bird.network.cz/` (Accessed on 25/06/2018).

[9] Kevin Butler, Toni R Farley, Patrick McDaniel, and Jennifer Rexford. A survey of BGP security issues and solutions. *Proceedings of the IEEE*, 98(1):100–122, 2010.

[10] Arthur Callado, Carlos Kamienski, Géza Szabó, Balázs Péter Gero, Judith Kelner, Stênio Fernandes, and Djamel Sadok. A survey on internet traffic identification. *IEEE communications surveys & tutorials*, 11 (3), 2009.

[11] Nikolaos Chatzis, Georgios Smaragdakis, Jan Böttger, Thomas Krenc, and Anja Feldmann. On the benefits of using a large IXP as an Internet vantage point. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 333–346. ACM, 2013.

[12] Marco Chiesa, Christoph Dietzel, Gianni Antichi, Marc Bruyere, Ignacio Castro, Mitch Gusat, Thomas King, Andrew W Moore, Thanh Dang Nguyen, Philippe Owezarski, et al. Inter-domain networking innovation on steroids: empowering ixps with SDN capabilities. *IEEE Communications Magazine*, 54(10): 102–108, 2016.

[13] B. Claise, B. Trammell, and P. Aitken. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. STD 77, IETF, September 2013.

[14] Jakub Czyz, Michael Kallitsis, Manaf Gharaibeh, Christos Papadopoulos, Michael Bailey, and Manish Karir. Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 435–448. ACM, 2014.

[15] DE-CIX. Blackholing - DE-CIX. Available at `https://www.de-cix.net/en/de-cix-service-world/blackholing` (Accessed on 11/07/2018).

[16] Christoph Dietzel, Anja Feldmann, and Thomas King. Blackholing at IXPs: On the Effectiveness of DDoS Mitigation in the Wild. In *International Conference on Passive and Active Network Measurement*, pages 319–332. Springer, 2016.

[17] Benoit Donnet and Olivier Bonaventure. On BGP communities. *ACM SIGCOMM Computer Communication Review*, 38(2):55–59, 2008.

[18] W. Eddy. TCP SYN Flooding Attacks and Common Mitigations. RFC 4987, IETF, August 2007.

[19] Dino Farinacci, Tony Li, Stan Hanks, David Meyer, and Paul Traina. Generic Routing Encapsulation (GRE). RFC 2784, IETF, March 2000.

[20] FastNetMon. FastNetMon DDoS detection tool. Available at `https://www.fastnetmon.com/` (Accessed on 25/06/2018).

[21] Seyed Kaveh Fayaz, Yoshiaki Tobioka, Vyas Sekar, and Michael Bailey. Bohatei: Flexible and Elastic DDoS Defense. In *USENIX Security Symposium*, pages 817–832, 2015.

[22] Nick Feamster, Jennifer Rexford, Scott Shenker, Russ Clark, Ron Hutchins, Dave Levin, and Josh Bailey. SDX: A software defined internet exchange. *Open Networking Summit*, page 1, 2013.

[23] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. BCP 38, IETF, May 2000.

[24] Linux Foundation. Production Quality, Multilayer Open Virtual Switch. Available at `https://www.openvswitch.org/` (Accessed on 28/06/2018).

[25] Google. reCAPTCHA: Easy on Humans, Hard on Bots. Available at `https://www.google.com/recaptcha/` (Accessed on 03/07/2018).

[26] ABN AMRO Group. Service temporarily disrupted by DDoS attacks, Jan 2018. Available at `https://www.abnamro.com/en/newsroom/newsarticles/2018/service-temporarily-disrupted-by-ddos-attacks.html` (Accessed on 07/06/2018).

[27] Arpit Gupta, Laurent Vanbever, Muhammad Shahbaz, Sean P Donovan, Brandon Schlinker, Nick Feamster, Jennifer Rexford, Scott Shenker, Russ Clark, and Ethan Katz-Bassett. SDX: A software defined internet exchange. *ACM SIGCOMM Computer Communication Review*, 44(4):551–562, 2015.

[28] Ben Herzberg, Dima Bekerman, and Igal Zeifman. Breaking Down Mirai: An IoT DDoS botnet analysis. *Incapsula Blog, Bots and DDoS, Security*, 2016.

[29] Chang-Jung Hsieh and Ting-Yuan Chan. Detection DDoS attacks based on neural-network using Apache Spark. In *Applied System Innovation (ICASI), 2016 International Conference on*, pages 1–4. IEEE, 2016.

[30] Huawei. Huawei DDoS Protection Systems Huawei products. Available at `https://e.huawei.com/en/products/enterprise-networking/security/anti-ddos` (Accessed on 12/06/2018).

[31] Marit Network Inc. IRR - Internet Routing Registry. Available at `http://www.irr.net/` (Accessed on 03/07/2018).

[32] iPerf. iPerf - The TCP, UDP and SCTP network bandwidth measurement tool. Available at `https://www.iperf.fr/` (Accessed on 29/06/2018).

[33] JavaPipe. 35 Types of DDoS Attacks Explained, Jan 2018. Available at `https://javapipe.com/ddos/blog/ddos-types/` (Accessed on 09/07/2018).

[34] Kirk Lougheed and Jacob Rekhter. Border gateway protocol (bgp). RFC 1105, RFC Editor, June 1989. URL `http://www.rfc-editor.org/rfc/rfc1105.txt`. `http://www.rfc-editor.org/rfc/rfc1105.txt`.

[35] P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch, and D. McPherson. Dissemination of Flow Specification Rules. RFC 5575, IETF, August 2009.

[36] Vincenzo Matta, Mario Di Mauro, and Maurizio Longo. DDoS attacks with randomized traffic innovation: botnet identification challenges and strategies. *IEEE Transactions on Information Forensics and Security*, 12(8):1844–1859, 2017.

[37] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[38] MSK-IX. Route Server :: MSK-IX Knowledge Base. Available at `https://kb.msk-ix.ru/en/ix/services/route-server/#blackhole` (Accessed on 11/07/2018).

[39] RIPE NCC. RPKI Validator API - RIPE Network Coordination Centre, 2016. Available at `https://www.ripe.net/support/documentation/developer-documentation/rpki-validator-api` (Accessed on 08/07/2018).

[40] NET-IX. NetIX Blackholing. Available at `https://www.netix.net/services#blackholing` (Accessed on 11/07/2018).

[41] Cisco IOS NetFlow. Introduction to Cisco IOS NetFlow - A Technical Overview, 2012. Available at `https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html` (Accessed on 18/06/2018).

[42] NetScout. DDoS & Network Visibility Solutions — NETSCOUT Arbor. Available at `https://www.netscout.com/arbor` (Accessed on 12/06/2018).

[43] P. Phaal, S. Panchen, and N. McKee. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks. RFC 3176, IETF, September 2001.

[44] NBIP Stichting Nationale Beheersorganisatie Internet Providers. NBIP DDoS Data Report 2017 now available. Available at `https://www.nbip.nl/nl/2018/05/16/nbip-ddos-data-report-2017-now-available/` (Accessed on 02/07/2018).

[45] NBIP Stichting Nationale Beheersorganisatie Internet Providers. NaWas - the not-for-profit National Scrubbing Center against DDoS attacks, 2018. Available at `hhttps://www.nbip.nl/nawas/` (Accessed on 21/06/2018).

[46] Radware. DDoS Services: Cloud Security Products and Solutions — Radware. Available at `https://www.radware.com/` (Accessed on 12/06/2018).

[47] Philipp Richter, Georgios Smaragdakis, Anja Feldmann, Nikolaos Chatzis, Jan Boettger, and Walter Willinger. Peering at peerings: On the role of IXP route servers. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 31–44. ACM, 2014.

[48] Christian Rossow. Amplification hell: Revisiting network protocols for ddos abuse. In *NDSS*, 2014.

[49] Fabrice J Ryba, Matthew Orlinski, Matthias Wählisch, Christian Rossow, and Thomas C Schmidt. Amplification and DRDoS Attack Defense–A Survey and New Perspectives. *arXiv preprint arXiv:1505.07892*, 2015.

[50] José Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, and Aiko Pras. BootersAn analysis of DDoS-as-a-service attacks. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 243–251. IEEE, 2015.

[51] sFlow.org. sFlow.org - Making the Network Visible. Available at `https://sflow.org/` (Accessed on 18/06/2018).

[52] Kotikalapudi Sriram, Doug Montgomery, Oliver Borchert, Okhee Kim, and D Richard Kuhn. Study of bgp peering session attacks and their impacts on routing performance. *IEEE Journal on Selected Areas in Communications*, 24(10):1901–1915, 2006.

[53] Henk Steenman. A simple and robust solution for protecting critical infrastructures against DDoS attacks, Mar 2018. Available at `https://ams-ix.net/newsitems/325` (Accessed on 05/07/2018).

[54] Jessica Steinberger, José Jair Santanna, Evangelos Spatharas, Hendrik Amler, Niklas Breuer, Kristian Graul, Benjamin Kuhnert, Ulrike Piontek, Anna Sperotto, Harald Baier, et al. Ludo - kids playing Distributed Denial of Service. 2016.

[55] Cisco Systems. Remotely triggered Black Hole Filtering - Destination based and Source based, 2005. Available at `https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf` (Accessed on 15/06/2018).

[56] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. Dnssec and its potential for ddos attacks: a comprehensive measurement study. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 449–460. ACM, 2014.

[57] Drashti Vashi and Varshkumar Patel. Security, Privacy and Trust Issues in Internet of Things. *International Journal of Innovations & Advancement in Computer Science*, 2017. ISSN 2347 - 8616.

[58] Shaun Waterman. Arbor: DDoS attacks growing faster in size, complexity (Jan 2018), Jan 2018. Available at `https://www.cyberscoop.com/ddos-attacks-growing-arbor-networks/` (Accessed on 07/06/2018).

[59] Saman Taghavi Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, 15(4):2046–2069, 2013.

[60] Boyang Zhang, Tao Zhang, and Zhijian Yu. DDoS detection and prevention based on artificial intelligence techniques. In *Computer and Communications (ICCC), 2017 3rd IEEE International Conference on*, pages 1276–1280. IEEE, 2017.

[61] Hubert Zimmermann. OSI reference model–The ISO model of architecture for open systems interconnection. *IEEE Transactions on communications*, 28(4):425–432, 1980.