DDoS Mitigation via Regional Cleaning Centers

Sharad Agarwal[†]
University of California, Berkeley
sagarwal@cs.berkeley.edu

Travis Dawson
Sprint ATL
tdawson@sprintlabs.com

Christos Tryfonas[†]
Kazeon Systems, Inc.
tryfonas@kazeon.com

Abstract— **We propose to address the problem of Distributed Denial of Service (DDoS) attacks at the ISP level by introducing the concept of regional cleaning centers. These centers perform the necessary traffic cleaning when a set of destination hosts is under attack. We describe the components of such centers, requirements for their operation, and deployment scenarios that present issues in diverting and redirecting traffic to and from them. Finally, we evaluate some of these methods using an experimental cleaning center and demonstrate the metrics associated with the usability of each method. Our results indicate that cleaning centers are a viable option for traffic cleaning as well as for other applications such as traffic logging, provided that their impact on traffic dynamics are considered during a network-wide traffic engineering process.**

I. Introduction

An increasing number of services and applications rely on the Internet today, not only for simple tasks but also for complex and critical ones. Along with this increasing reliance on the Internet, new problems have appeared. Denial of Service (DoS) attacks are now a prominent issue due to their ability to disrupt services and communication infrastructure [1]. Over the last few years, DoS attacks have evolved from a nuisance to a real and constant threat.

A DoS attack consumes the resources of a remote host and/or network in an effort to deny the use of those resources to legitimate users. A variety of DDoS attack techniques exist [2]. Logic attacks exploit existing software flaws to cause remote hosts to either crash or significantly degrade in performance. Such attacks can sometimes be prevented by either upgrading faulty software or filtering particular packet sequences. A flooding attack inundates the victim with so much additional malicious traffic that its network connection or its servers get saturated. The result is a network and/or end-system that is no longer able to respond to normal requests in a timely manner, effectively disabling the service.

In some cases, a single host carrying out a flooding attack can have a devastating effect on a victim. Even more damaging is an attack that is amplified by the use of multiple hosts (also called *zombies*) to launch a coordinated attack against a single victim. This type of attack is called a Distributed Denial of Service (DDoS) attack. Zombies are often obtained by compromising unsuspecting end hosts by means of network worms that exploit certain vulnerabilities [3].

A. Addressing DDoS Attacks

Although DDoS attacks can sometimes have predictable effects, it is still difficult to mitigate them. The main tactics can be classified as either proactive or reactive. In the former case, the focus is on establishing a framework so that the attack cannot block legitimate users from accessing resources [4], [5], [6]. These techniques may include authorizing only legitimate users to access protected servers and applying packet filters in routers to drop spoofed IP packets. The reactive tactic is followed by most end systems and intermediate networks today, and can be summarized as having the following steps [7]: (i) preparation, (ii) identification, (iii) classification, (iv) traceback, (v) reaction, and (vi) post mortem.

Preparation of a network includes tool creation and testing, the development of the procedures for handling of incidents, and the training of the response team. This may include the activation of ingress filtering [8] and unicast reverse path forwarding (uRPF) [9]. This blocks spoofed packets originating from inside the local network or transiting it. To identify and classify attacks, various techniques such as anomaly detection [10] and signature-based detection [11], [12] are used. Traceback attempts to find the network ingress points where the attacks are coming from (practical IP traceback [13], backscatter traceback [14]). It is often combined with the reaction step as in the pushback scheme [15]. CenterTrack [16] is a traceback scheme that uses tunnels from all the edge routers in an ISP to a set of routers capable of performing traffic accounting and auditing. However, it does not consider large DDoS attacks, the impact on SLAs, nor any issues surrounding the deployment and selection of multiple units. Reaction is the step at which the actual mitigation takes place. Finally, the post mortem stage applies forensics techniques, which may involve the manual analysis of collected data, to improve the preparation step.

In this paper, we focus on the reaction step. Here, mitigation is generally achieved through two forms of filtering : (i) router based filtering and/or (ii) specialized filtering devices.

B. Router Based Filtering

The most commonly used method to block an attack is the customization of router filters, also referred to as *Access Control Lists (ACL's)*. These filters can block traffic that matches certain rules applied on the headers of the packets. Router vendors provide extensions to their ACL rules that allow for the more fine-grained definitions needed to weed out malicious traffic. The different traceback methods can be used to select the routers at which the filters should be applied. The goal is to apply the least number of filters necessary to mitigate the attack. Typically, the filter list is static and is applied on routers at the edge of the network. However, on some router implementations, lengthy filters can significantly slow down packet forwarding. Given the restrictions of ACL rules and extensions, the filters may have to block all traffic to a targeted machine. Although this method can save network resources and protect the victim, the attack

[†] This work was done while the authors were at Sprint ATL.
The views expressed in this work do not necessarily represent those of the Sprint Corporation.

still has the effect of shutting down valid traffic. Traceback may require some time before filters can be applied at the appropriate places, and some traceback methods require router software modifications.

A more sophisticated method using packet shaping techniques can also be employed. This method uses queues to rate-limit traffic destined for the machines under attack. For example, all the traffic from a particular source address might be allowed to consume at most a fraction of the available bandwidth. Though this technique can be useful, an attacker can defeat it by adding more *zombies* to an attack, each with a different source address. Packet shapers alone are not the answer. They can be a useful part of a DDoS defense but they need to be coordinated with other DDoS techniques in order to be effective.

C. Specialized Filtering Devices

Specialized filtering devices, which we describe in more detail in the next section, are typically used in two configurations in an enterprise network. In the *inline* method, the device is placed directly in the path of the incoming traffic, just before the ingress traffic hits the edge router of the enterprise network. Here the device is always on, continually filtering packets with known malicious payload signatures and anomalous behavior. A variety of anomaly detection, filtering, and rate shaping methods may be employed by this hardware. In the *on demand* setting, the device may sit on a separate port of the edge router, and ingress traffic may get shunted through this port if an attack is suspected.

While these devices are starting to become more popular in enterprise networks, their current use is lacking in many respects. Firstly, since these devices are on the enterprise network side, DDoS attacks that attempt to saturate under-provisioned edge links to ISP customers will still be successful. Even if the malicious traffic is successfully filtered by the device, since the network connection is saturated by this traffic, legitimate traffic cannot flow through.

Secondly, such a deployment results in a single point of failure. If the filtering device malfunctions, malicious traffic may be let in or all traffic may get blocked. Placing multiple devices can get prohibitively expensive for small enterprise networks.

Thirdly, this technique requires all enterprise networks to deploy filtering devices before DDoS attacks can become a thing of the past. This cannot easily scale to the large number of enterprise networks that exist today and those that are yet to join the Internet.

D. Cleaning Centers

In this work, we present a technique to address all three of these drawbacks. We propose that large numbers of these devices be deployed in a *cleaning center*, and multiple cleaning centers be deployed inside ISPs. By deploying them inside ISP backbones, we are no longer victim to DDoS attacks saturating under-provisioned edge links. We are no longer placing the burden of DDoS attack mitigation with large numbers of enterprise networks, but instead placing the burden with the fewer numbers of ISPs. Further, large numbers of devices and cleaning centers in an ISP are amortized among many enterprise customers. A single point of failure will no longer exist in a well designed solution.

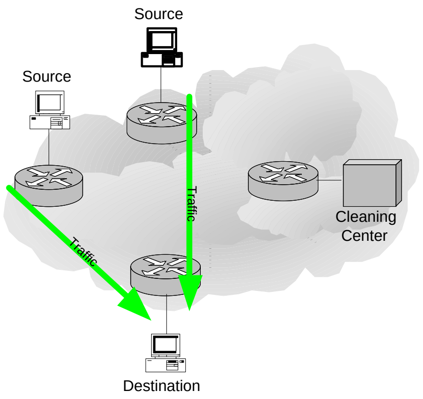

Fig. 1. Normal Network Operation

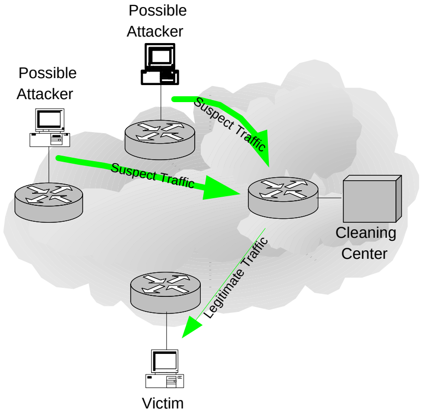

Fig. 2. DDoS Attack Operation

This deployment requires the consideration of traffic *diversion* and *redirection* techniques. During normal operation, traffic will flow across an ISP's network from multiple sources to a particular destination, as in Figure 1. When an attack occurs, suspect traffic to this destination is diverted to a cleaning center in the ISP, as shown in Figures 2 and 3. When this traffic is cleaned by one or more specialized filtering devices in the center, the legitimate traffic is redirected to the destination.

This method takes advantage of the fact that the capacity of the backbone is large. Thus, it can absorb the attack traffic without the need to install router filters which could block all traffic to the victim. Apart from traffic cleaning, there are other applications that could benefit from the cleaning center concept. These include traffic logging, sinkholing, blackholing, monitoring of misbehaving customers or peers, and selective traffic analysis for re-engineering of service level agreements (SLAs).

In this work, we focus on issues in the deployment of filtering devices, not on the effectiveness of the individual devices in blocking malicious traffic. Our contribution is the introduction of the concept of regional cleaning centers for DDoS mitigation in a large IP backbone network. We describe an architecture for a cleaning center and the various metrics under which such centers should be designed. We examine several techniques for

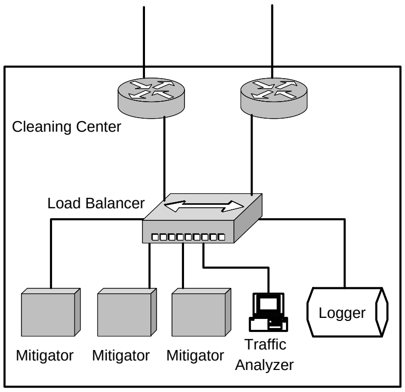

Fig. 3. Cleaning Center

addressing the diversion and redirection necessary for the operation of cleaning centers. Even though our architecture is targeted for a large network, for simplicity we evaluate the impact of some of these techniques in a limited laboratory testbed. We use a commercial specialized filtering device and commercial routers typically used in a large ISP. We find that when an application server is under attack, a cleaning center can dramatically improve the performance to the application service. However, performance during mitigation is lower than when no attack and mitigation is employed. To the best of our knowledge, the issues surrounding cleaning center deployment in an ISP setting have not been addressed in the prior literature.

The rest of the paper is as follows: in Section II, we elaborate on the concept of cleaning centers and present an architecture. We describe issues involved in re-engineering customer SLAs in Section III. We analyze several methods to achieve route diversion and redirection in Section IV. We present our results from a sample cleaning center in Section V. Finally, we conclude the paper in Section VI by summarizing the main points and providing areas for further exploration.

II. Cleaning Center Architecture Components

In this work, we focus on the architecture, operational requirements and routing support for DDoS attack mitigation. However, the architecture that we present is intentionally designed to also support additional applications such as traffic analysis that we describe at the end of this section.

Traffic enters the cleaning center (*ingress traffic*) from various parts of the network, and some traffic leaves the cleaning center (*egress traffic*) toward the destination. Depending on the characteristics of the traffic, the egress traffic may be all, none or some fraction of the ingress traffic. During operation, all traffic to a particular destination *must* go through a cleaning center. Due to this requirement, special routing techniques need to be employed, which we present in a later section. In this section, we briefly describe the issues involved, but it is beyond the scope of this work to consider hardware design issues.

A. Structure

A cleaning center is a collection of devices and network links housed within a single facility, such as a building or PoP (point of presence) or switching center. These devices include routing and switching hardware, traffic logging and analysis hardware and DDoS mitigation hardware.

A.1 DDoS Mitigation Hardware

Three kinds of DDoS mitigation hardware are currently available on the market. We use the term *filter suggestor* to describe products that analyze DDoS traffic and identify patterns in the attack traffic. Based on this fingerprint, filters are applied in already deployed network routers and firewalls, usually in the form of ACLs (access control lists). We use the term *blackholers* to describe products that fingerprint the attack traffic and inject routing announcements to drop that traffic. These products may drop traffic immediately upon reaching any router inside the domain, or forwarding it to a central location that drops the traffic.

We use the term *inline scrubbers* to refer to products that inspect both malicious and legitimate traffic, identify the legitimate traffic, and allow only that traffic to exit the device. These products use passive techniques, such as inspection of the packet headers and content. They also use active techniques, such as completing TCP handshakes before allowing interaction with the destination. Techniques based on the SYN cookie method are also popular which analyze the TCP sequence number in SYN packets. In this work, we focus on the inline scrubbers.

Many such devices exist on the market today [1]. Top Layer's Attack Mitigator IPS is an inline scrubbing device. Arbor Networks' Peakflow SP provides filter suggesting functionality. Riverhead Networks' Guard provides inline scrubbing functionality. Mazu Networks' Enforcer and netZentry's FloodGuard provide filter suggesting capabilities. Many of these devices use ASIC based solutions to achieve gigabit and higher speeds on Ethernet interfaces. With ISP backbones built on many OC-192 links, it is clear that many such devices will be needed across all the cleaning centers to handle simultaneous DDoS attacks on multiple customers.

A.2 Router Hardware

In order to receive traffic at the cleaning center, one or more switches or routers are needed to interface with the rest of the network. The capacities of the ingress link(s) and the egress link(s) should not present bottlenecks to the amount of traffic that can be handled by the center. It is more likely to be limited by the traffic handling capabilities of each unit of DDoS mitigation hardware. A local area network is needed to connect one or more of the mitigation units to the switches or routers. The center needs to handle egress volumes up to the amount of ingress volume that is provisioned.

To divert customer traffic to the cleaning center, routing changes in the network will be needed. The routers that interface the cleaning center with the rest of the network will inject the changes. This will cause routing table entries at network ingress points to point to the cleaning center ingress point for the victim destination addresses. These changes are initiated when an attack is detected, which can be automated with detection hardware that we do not address in this work. Additional routes are

[1] http://www.toplayer.com, http://www.riverhead.com, http://www.netzentry.com, http://www.arbornetworks.com, http://www.mazunetworks.com

needed to send the clean egress traffic from the cleaning center to network egress points. Otherwise, this traffic would loop back to the ingress of the cleaning center. We describe multiple techniques for performing this rerouting in the next section.

B. Multiple DDoS Mitigation Devices and Cleaning Centers

B.1 Load Balancing

Due to the limited traffic handling capabilities of current DDoS mitigation hardware, multiple such units are needed in a cleaning center. Thus, when traffic enters a center, it is split across the multiple mitigation units. In doing so, two main constraints exist. Firstly, packets from an end-to-end application flow should not be split across multiple devices. Packets through different devices may experience different latencies and that may lead to packet reordering, which can be detrimental to some applications. Secondly, some forms of DDoS attack signature detection, filtering and scrubbing techniques may perform poorly if a device does not see all the ingress traffic. Techniques that correlate information across packets, such as characterizing source address distributions may suffer. Active techniques that employ SYN cookies will not work if packets from a particular source address and port to another destination address and port do not always traverse the same device.

This ingress load balancing is performed by the ingress routers. Each ingress router's path to each mitigation device will have an equal cost as in an ECMP (equal cost multi-path) configuration. Typically, routers employ 5-tuple hashing to determine which path each packet should go to, which considers the source IP address, destination IP address, source IP port, destination IP port and protocol type. This is sufficient to avoid packet reordering and to ensure that packets from the same flow go to the same device. The resulting clean traffic from the multiple DDoS mitigation units is not combined in any special way before egressing the center since few applications are affected by reordering of packets across different flows.

Beyond having multiple mitigation units in a center, multiple cleaning centers are needed in large ISPs. Large ISPs today have networks spanning the globe with thousands of customers. A customer can connect via one or more OC-3, OC-12 or OC-48 links. The backbones of such ISPs use OC-48 and OC-192 links to transport the large volumes of traffic between all the customers and peers. Even if a very large centralized cleaning center can be architected to withstand a DDoS attack toward multiple customers at the same time, the latency penalty experienced by traffic going through such a center would be enormous. Thus, multiple cleaning centers are needed.

B.2 Cleaning Center Placement and Selection

If multiple cleaning centers are to be deployed in a network, the first issue is how to place them. Let us consider distance in terms of network latency. Ideally, each suspect packet should not traverse a new path via a cleaning center that has a higher latency than the original path. Thus, a cleaning center should be available anywhere along each of the paths between every network ingress point and every network egress point. Costs may prohibit placing cleaning centers in all possible locations inside a network. Given a limited number of cleaning centers, the additional latency on the ingress path and on the egress path need to be minimized.

The goal is to minimize the impact on the Service Level Agreement (SLA) during attack mitigation. SLAs are typically defined as the time delay between two geographic points in the network, such as the average latency between San Francisco and New York, or the average latency across the Atlantic Ocean. Thus, the optimization will place centers in such a way as to minimize the difference between the latency under attack mitigation and the promised SLA latency. This needs to run over all possible traffic routes - i.e., minimizing the worst latency increase. The factors include the location of the network ingress points, egress points for each customer, the number of mitigation devices in each center, the traffic load that each device can handle, the traffic volumes between ingress and egress points and the candidate cleaning center locations. Worst case scenarios will be considered when running this optimization.

Upon placing centers, a technique for selecting them is needed. No center should be given more traffic than it can handle, else queueing delay will significantly impact legitimate traffic and the center can itself become a victim of the attacks. The ingress and egress links to and from each cleaning center should be provisioned to adequately handle this traffic. The ideal technique will consider the load that is currently experienced by each center and its limit before assigning more traffic to any one of them. Attack volumes may change and this load may vary over time. It will migrate attack traffic to a different cleaning center after some time, or distribute the load to a particular victim across multiple centers. This is further complicated by the fact that network customers may also specify the egress links to use for particular traffic through various mechanisms such as MED (multi-exit discriminator) available in BGP (border gateway protocol) [17]. A simple solution is desirable and it will be tied directly to the re-routing techniques used to divert suspect traffic through a cleaning center. We will re-visit this issue in a later section devoted to re-routing techniques.

C. DDoS Attack Detection

This work is focused on cleaning traffic and does not address the detection of DDoS attacks. Our cleaning center solution needs a detection mechanism. We assume that a solution independent of the cleaning center architecture is deployed. For example, each customer may employ their own detection hardware that is customized for the services it offers on the network. The customer then uses some form of signaling to request the ISP to initiate traffic cleaning. This signaling will have to occur out-of-band as the customer's network connection will be heavily congested during an attack. The telephone network may be a slow but generally reliable solution.

However, upon commencing cleaning center mitigation, a mechanism is needed to detect when the attack has subsided. Since only legitimate traffic may be flowing to the customer, it can no longer detect if the attack is still in progress. This is best handled by the cleaning centers themselves. SNMP (Simple Network Management Protocol) statistics are maintained by the routers in each cleaning center. When the volume of traffic has subsided, and the suspect traffic volume has been the same as the cleaned traffic volume for a significant period of time, cleaning can be turned off. It should be noted that our cleaning center solution is a "stop-gap" measure. It does not prevent the attack - it filters out the malicious traffic. It gives the ISP and/or the customer additional time to locate and stop the attackers, during which the customer's services continue to be available.

D. Other Applications

In this work, we describe the cleaning center architecture and associated routing techniques for DDoS mitigation. However, this system lends itself to other applications as well.

One such application is traffic logging. In addition to DDoS mitigation hardware, monitoring hardware can be installed that captures packet headers, full packet contents or aggregate statistics [18]. This is useful for debugging network or application performance problems. For example, a customer can complain that an unusually high packet drop rate is being experienced. The ISP can engage logging of this traffic at a cleaning center near the network ingress points and at a cleaning center near the network egress points and compare the packet drop rate across the ISP's network. In a similar fashion, this can be used to reengineer SLAs if long term traffic patterns have changed, to characterize backbone traffic for network provisioning and to identify misbehaving customers or peers. Traffic to or from unallocated addresses that should not sink legitimate traffic can be logged for analysis. The same techniques of ingress and egress routing support and load balancing across multiple logging devices and cleaning centers can be applied for these applications.

III. ISP Service Requirements

In order to be safe from DDoS attacks, a network entity has to rely on a DDoS mitigation solution that can handle the largest foreseeable attack. Such a solution is prohibitively expensive for small network entities since many DDoS mitigation devices, routers and links need to be deployed for a relatively rare event. However, across multiple network entities, the relatively rare event becomes relatively common. It is more feasible to amortize such a large investment across many network entities. A natural aggregation point for deploying such a shared infrastructure is an ISP.

Since all or most traffic to these entities passes through their ISPs, if they were to deploy regional cleaning centers, it would relieve their customers of the burden of DDoS attack mitigation. The customers will save the expense of building the same service in each of their networks. For the ISPs, additional expense is needed to deploy cleaning centers and to administer the additional equipment. However, this can be deployed in an incremental fashion. As more customers purchase the service, and attacks become more frequent and larger, more cleaning centers will be deployed, and more mitigation devices will be added to existing ones. In addition to amortizing this equipment over many possible customers, it will be amortized across other applications such as traffic logging. In this work, we primarily focus on the solution for an ISP deployment scenario.

SLAs (service level agreements) that are promised today to customers by ISPs are often violated during large DDoS attacks due to the disruption in typical network operation. As we indicated in the previous section, even with our regional cleaning center approach, additional latency will be experienced by traffic being cleaned. Thus, with our approach, SLAs will be different. Existing SLAs can continue to be guaranteed under normal operation. A second SLA under attack conditions will be offered that provides "degraded" service guarantees instead of the disrupted service that is offered today. We now list the issues that will be addressed when defining this degraded SLA.

- **Impact on SLA** - Several metrics are typically involved in existing SLAs between an ISP and its customers. The DDoS mitigation solution must be designed to minimize the impact on these metrics. For example, splitting suspect traffic across multiple mitigation devices or cleaning centers may result in packet reordering. Ingress re-routing, inline scrubbing and egress re-routing of suspect traffic will add more latency to packets. If the capacity of the cleaning center solution is inadequate to handle all of a customer's traffic, then more stringent bandwidth constraints will exist than those specified in the original SLA. Unnecessary packet loss of valid traffic will occur. Imperfect DDoS mitigation devices inside cleaning centers can misinterpret valid traffic as attack traffic and drop it, thereby further reducing the bandwidth available to a customer. All of these negative impacts must be estimated during design, minimized and then specified in the SLA.
- **Impact on applications** - In addition to the SLA metrics that change during DDoS attack mitigation such as additional latency that may impact applications, other impacts can be felt. Some of the re-routing techniques that we describe in the next section require tunneling mechanisms. Tunneling mechanisms typically add additional headers to IP packets, which may cause large packets to be fragmented. This will impact application performance unless the tunneling routers are configured to allow large packets. Due to this encapsulation, TTL (time to live) values in ICMP packets will not be properly decremented when going through a tunnel. Thus, traceroutes will report erroneous information.
- **Effectiveness of mitigation** - The effectiveness of the DDoS mitigation will need to be specified in the SLA for this new type of service. It is unlikely that a mitigation device available today can filter all malicious packets in all forms of attacks. As we described earlier, splitting suspect traffic across multiple devices or cleaning centers may further reduce their effectiveness. This important performance metric needs to be measured and quantified on the SLA promised to a customer. This is especially difficult to do since different forms of DDoS attacks appear over time.
- **Speed of mitigation** - In this work, we do not address the issue of attack detection. This can either be handled by detection mechanisms in the ISP or in the customer network. In the latter case, an out of band notification is needed for the ISP to initiate mitigation. The time between notification and activation of cleaning is a critical component of the SLA. This will primarily be the time for ingress or egress re-routing to occur, which we describe in the next section. This is likely to be in the order of seconds.
- **Impact on ISP infrastructure** - There are two kinds of changes that occur to the ISP infrastructure during DDoS mitigation. Firstly, router configurations change so that suspect traffic is diverted and clean traffic is delivered. This change may require human operator intervention. The different re-routing

techniques that we describe in the next section impose different constraints in this respect. Also, a side effect on the routers is an increase in router CPU loads both due to the configuration change and possibly continuously during the re-routing. Router CPU loads is an important side effect to avoid since high loads can be detrimental to performance and in extreme cases can result in router downtime. The second kind of change that can occur during DDoS mitigation is a change in traffic patterns across an ISP's backbone. Since traffic is being diverted from the normal paths between network ingress and network egress points to paths via cleaning centers, link loads across the network can change. Some links will experience less traffic while others will experience more traffic. Some links may get overloaded, resulting in degraded performance for both the victim and customers not directly targeted by an attack. When provisioning the network to meet the SLA, these factors need to be considered.

- **DDoS of the cleaning center** - Since the cleaning center is designed to mitigate a DDoS attack toward a customer by absorbing all the suspect traffic, it has to be designed to avoid becoming susceptible itself. This can happen in at least three ways. Firstly, more traffic than can be handled may get redirected to a cleaning center. This can be avoided by more carefully balancing traffic among cleaning centers. As a failsafe, the ingress router in each cleaning center should limit the traffic it sends to each mitigation device, dropping any excess traffic. Secondly, the cleaning center can be attacked directly. If the IP addresses of the routers or mitigation devices in the cleaning center are known by an attacker, it may be possible to attack the center and render it useless in mitigating simultaneous attacks on customers. One way to prevent this is to use only private local address space (e.g. in the $192.168/16$ space) and ensure that ACLs or similar filters are enabled at the network ingress points that block traffic to these addresses. A third way is for an attacker to exploit the overhead of traffic cleaning. Every time an attack to a customer is detected, re-routing techniques need to be applied to send the traffic to a center. When the attack subsides, the techniques need to be deactivated. This incurs an overhead in reconfiguring routers. An attacker can potentially start and stop DDoS attacks for very short periods of time to many different customers to overload this router reconfiguration mechanism. Two dampening techniques need to be considered. As our results indicate, re-routing traffic for small amounts of attack traffic incurs too much overhead compared to the small detrimental impact on server response time. Thus, only upon detecting a large enough attack should cleaning be initiated. Further, once initiated, cleaning should proceed for some number of hours to dampen the configuration impact from rapid changes in attack patterns.
- **Effectiveness of post mortem** - Once the attack has subsided, re-routing can be canceled and traffic can return to the normal operating paths. However, customers will want details on the attack traffic to determine the source of the attack. This will aid in the prosecution of the attackers. Also, information about the kind of attack will be useful in improving the mitigation and detection devices. Logging techniques must be used to store enough information about the attack traffic to aid in this investigation. Details about the source address ranges used and common characteristics of the data payload and TCP/IP headers among the attack packets will be useful.

IV. Traffic Handling for Cleaning Centers

In the previous section, we described techniques for the design of individual cleaning centers, the placement of multiple centers in a network and the selection of a center for suspect traffic. The remaining design decision is that of transferring the suspect traffic to the cleaning centers, and the clean traffic to the egress links. Under normal operation, traffic flows from multiple network ingress links to a particular customer of the network via one or more egress links. The paths between the ingress and egress points are determined by the various routing protocols that networks employ. If this customer is under attack, the traffic will still flow between the same ingress and egress points. However, it will take different paths between these points - they will flow through cleaning centers. This requires changing the routing scenario in the network for the suspect traffic. Various techniques exist for re-routing that modify the existing routing tables or bypass them. Some have performance or usability limitations and some require particular protocols or routing equipment. We briefly examine some of the various techniques available and how they can be combined for DDoS mitigation. In this work, we do not attempt to cover all the possible re-routing techniques and combinations that can be applied, but instead cover most of the feasible ones.

A. Re-Routing Traffic

An AS (autonomous system) is made of hosts, routers and links, typically running an intra-domain routing protocol or IGP (Interior Gateway Protocol) such as IS-IS (Intermediate System to Intermediate System) [19] or OSPF (Open Shortest Path First) [20]. The IGP determines how a network entity (end host or router) inside the AS reaches another network entity in the same AS via intermediate hops. To reach entities outside the AS, the inter-domain routing protocol or EGP (Exterior Gateway Protocol) used today is the Border Gateway Protocol or BGP [17]. Each AS announces aggregate information for the entities in its network via eBGP (external BGP) to neighboring ASes. This is in the form of a routing announcement or routing update for one or more network prefixes. A network prefix is a representation of a set of IP addresses, such as $128.32.0.0/16$ for every address in the range $128.32.0.0$ to $128.32.255.255$. Through the path vector operation of eBGP, other ASes find out how to reach these addresses.

Large ASes such as ISPs may have multiple border routers that peer with other ASes using eBGP. In order to distribute these BGP routes among all the routers in a scalable fashion, iBGP (internal BGP) is typically used. An iBGP route indicates the destination network prefix as well as the border router address that can carry traffic to this destination. A neighboring AS, such as a customer of this ISP, may connect to the ISP at multiple points. The customer may indicate which egress point is preferred for which prefix through the use of MEDs (multiple exit discriminators) in BGP announcements. If preferences such as MEDs are not specified, iBGP will use the IGP cost to each of the valid egress points to determine the route to use. Thus, in iBGP, different parts of the network may use different routes to the same destination address, and a particular router may use different exit points for different addresses that belong to the same neighboring AS.

We now briefly describe techniques to alter how packets traverse the network. Instead of going from the ingress points to the egress points, some packets must go through cleaning centers. This change can be induced by making routing announcements for the victim prefixes, using iBGP or eBGP. Alternatively, tunneling can be employed, using L2TPv3, GRE or MPLS. Conceptually, it involves making a virtual link between two points in the network. Packets entering one end of the link will always exit the other end, short of a network partition. Some technique is needed to classify which packets need to be re-routed. In the case of iBGP or eBGP, routing is performed on prefixes and thus packets are classified based on their destination address. In the case of tunneling, more flexible PBR rules or MPLS labels can be used. An important point to note is that two re-routing steps are needed - the traffic *diversion* which moves traffic from the ingress points to cleaning centers; the traffic *redirection* which moves traffic from the cleaning centers to the egress points.

A.1 Initial Traffic Diversion

The goal of traffic diversion is to send suspect traffic to a cleaning center before it enters the victim's network. There are two points at which we can make this change - traffic can be diverted at all the possible ingress points to the network, or it can be diverted just before it exits the network to enter the victim's network.

There are advantages and disadvantages to each approach. For a particular customer network, there are many ingress points where suspect traffic can enter the ISP network. In contrast, there are typically few egress points where that traffic exits the ISP network to enter the customer network. For some techniques that we describe, it is easier to divert the traffic at the few egress points since it reduces the reconfiguration overhead. However, the cleaning center that will handle this traffic should be in the vicinity of the egress points. Otherwise, additional latency and traffic load will be experienced in sending that traffic back into the ISP's backbone to reach the cleaning center and then back out to the customer.

A.2 Final Traffic Redirection

Once the suspect traffic has entered a cleaning center and only valid traffic remains, it must be sent to the customer network. However, some customer networks may connect to the ISP at multiple points. Thus, valid traffic exiting a cleaning center may have a choice of multiple network egress points to go to. Picking the closest egress point may reduce latency, but may not be the best choice due to congestion. Some customers specify preferred exit points for certain prefixes through MED announcements in BGP. Some of the redirection techniques that we describe support this selection while others do not.

B. Diversion and Redirection Techniques

We now describe various re-routing techniques. Some can be applied for both diversion and redirection. Some can only be used for one step and require another technique for the second step. While any technique or combination of techniques can be used, there are a variety of factors that should be considered in selecting one:

- Amount of pre-DDoS preparation required
- Amount of reconfiguration required after DDoS detection
- Initial latency of re-routing technique
- Flexibility in allowing multiple cleaning centers
- Flexibility in allowing multiple egress points
- Amount of reconfiguration required after DDoS abatement

B.1 iBGP and eBGP

During normal operation, the iBGP routing table will indicate what the egress point(s) for a particular destination is. The IGP will determine the path used to reach it. One technique for diversion is to change the iBGP routing table so that the egress point is actually a cleaning center.

For this technique, some pre-DDoS preparation is needed. During the installation of every cleaning center, router configurations throughout the ISP network need to be modified. A new policy is needed that gives any iBGP route tagged with a BGP *community attribute* [17] of a cleaning center the highest priority.

Upon attack detection, the cleaning center routers needs to announce the victim prefixes with this special community. There may be a delay before all ingress points forward traffic to the cleaning center. The BGP protocol uses a timer called *minrouteadver* [17] that determines the minimum spacing between successive announcements. For iBGP, the default value for this timer is 5 seconds. For a flat iBGP network, the latency range can thus be 0 to 5 seconds. For a network that uses an iBGP RR (route reflector) hierarchy, the range can be between 0 and 15 seconds. Upon abatement, these routes can be withdrawn and normal network operation will continue.

Multiple cleaning centers can be supported in two different ways. Each cleaning center can be assigned a particular prefix. This way, load can be balanced across different centers. Alternatively, each cleaning center can announce the same victim prefixes. The ingress router for each of the cleaning centers will have the same loopback address. The IGP will pick the closest cleaning center to use. This is a form of anycast [21]. This technique will optimize only for the initial latency penalty (between the network ingress point and the cleaning center).

This is the simplest form of diversion, but cannot also be used for redirection. Since only one iBGP routing table exists inside an AS and traffic is routed by destination address, it is not possible to distinguish routes for suspect traffic versus clean traffic. Thus, one of the following routing techniques is needed for redirection.

Instead of using iBGP announcements, we can use eBGP announcements. The cleaning centers can masquerade as a separate private AS, where each regional cleaning center appears as a link to the ISP network. Again, suspect traffic can be segregated among cleaning centers by IGP cost or by destination prefix range. However, the initial latency can be higher. eBGP sessions use a default 30 second minrouteadver timer. Now the range is between 0 and 35 seconds for a flat iBGP hierarchy and 0 and 45 for a two level hierarchy. Other than simpler configuration management, this technique has no inherent advantage over the iBGP technique.

B.2 MPLS Tunnels

In MPLS (multiprotocol label switching) [22], packets are tagged with labels upon entering the MPLS region of the network and are subsequently routed based only on the labels. Instead of using a dynamic routing algorithm such as OSPF, a particular path for each label is pre-allocated in the network.

If an MPLS network is used, then the natural solution is to use MPLS for both diversion and redirection. One set of labels will divert traffic to the cleaning centers. The cleaned traffic can be tagged with the second set of labels. A different set of paths can be set up from the cleaning centers to the egress points. If traffic to each customer is tagged uniquely, then no pre-DDoS preparation is needed. Upon attack commencement, the paths for the labels need to be altered and the latency of making this change will depend on the network configuration tool used to set up the paths. The distribution of traffic among multiple cleaning centers and multiple egress points can be as flexible as the initial label assignment. Upon termination, the path can be restored to the original. This technique does offer significant advantages of flexibility and speed over the previous ones, but can only be applied to a network that uses MPLS for internal routing.

B.3 PBR and VRF

BGP / MPLS VPNs (virtual private networks) [23] can be used to also modify routing. In this technique, routers maintain multiple separate routing tables, which is also known as VRF (VPN routing and forwarding). As with typical routing, each table can have route filters that determine how routes enter the table and how they propagate to other routers and tables within the same router via BGP. In this fashion, traffic from a particular interface or customer or IP address can be routed via a customized routing table. This technique uses MPLS tunnels to keep this traffic routed via the alternate routing table throughout the network. PBR (policy based routing) [24] allows for a more flexible specification of routing policy for certain kinds of packets. PBR allows ACLs (access control lists) to be specified that identify certain classes of traffic (such as a particular destination address or protocol type). In this context, PBR rules are used to force certain traffic to use a particular VRF table.

This technique can be easily applied to ingress diversion. A fair amount of pre-DDoS preparation is needed. VRF tables are set up in all the routers in the network that send packets destined to any of the customers with DDoS mitigation service to the cleaning center. Upon attack detection, PBR rules are applied to all the ingress routers that force suspect traffic to use the VRF table. The initial latency can be significant since the configurations of all the ingress routers need to be changed. Each cleaning center can be assigned different prefixes or each ingress router can send it's traffic to a different cleaning center. Upon termination of the attack, this PBR configuration can be removed from the ingress routers. Compared to the iBGP diversion method, this technique requires configuration changes to routers upon DDoS detection, which can be a slow and cumbersome process.

When using this technique for diversion, normal routing can be used for the final redirection. Valid traffic exiting the cleaning centers can use the normal routing table instead of the VRF table and be routed normally to the egress points. Alternatively, we can use iBGP routing announcements for diversion and this PBR-VRF technique to redirect traffic from the cleaning center to the egress points.

B.4 PBR and L2TPv3 Tunnels

L2TPv3 (layer 2 tunneling protocol version 3) [25] is a technique that can be used to create tunnels to bypass normal network routing. UTI (Universal Transport Interface) is a Cisco proprietary pre-standard implementation of L2TPv3. It allows for the creation of a tunnel across a packet switched network that looks like a layer-2 link to the two ends of the tunnel. At the source end of the tunnel, layer-2 frames are encapsulated into L2TPv3 tunnel headers followed by an IPv4 header (if going over an IP network). This packet gets delivered normally through the network to the destination which is the other end of the tunnel. At that end, the router will strip off the IPv4 and L2TPv3 headers and get back the layer-2 frame. However, there are limitations to using L2TPv3. In some Cisco routers, the number of tunnels that can be set up using UTI is limited to 1023. Due to the encapsulation, the MTU (maximum transmission unit) is reduced by 32 bytes (12 for the additional UTI header and 20 for the additional IPv4 header). Also, some Cisco routers may require additional hardware or software upgrades to use UTI.

This PBR-L2TPv3 technique can be used for diversion. Before a DDoS attack, tunnels are set up from all ingress routers to each cleaning center. After a DDoS attack is detected, PBR ACL rules are configured on all ingress routers to push traffic destined to the suspect prefixes through one or more tunnels. Different tunnels can be used to segregate traffic by router location or victim prefix to multiple cleaning centers. The initial latency will be high since router configuration changes are required. During diversion, additional latency may be experienced due to the encapsulation and decapsulation required by L2TPv3. Upon termination of the attack, the ACL rules can be removed. As we described before, there are limitations to the number of tunnels, the MTU size and router hardware and software required.

When using this technique for diversion, normal routing can be used for the final redirection. Valid traffic exiting the cleaning centers can use the normal routing table to get to the egress points. Alternatively, we can use iBGP routing announcements for diversion and this PBR-L2TPv3 technique to redirect traffic from the cleaning center to the egress points. In this case, tunnels are created between the cleaning centers and the egress points to all the victim customers. However, it may be difficult to adhere to MED (multi exit discriminator) values that customers specify in their BGP announcements.

B.5 PBR and GRE Tunnels

Another tunneling technique is GRE (generic routing encapsulation) [26]. Unlike L2TPv3, GRE does not create a virtual layer-2 connection. Instead, packets are encapsulated inside a new IPv4 packet with a different destination address. At the destination, the packets can be decapsulated. However, the GRE header requires 8 bytes and the additional IPv4 delivery header requires 20 bytes which reduces the MTU [27], as in L2TPv3. However, for both GRE and L2TPv3, the routers inside the ISP can be reconfigured to allow MTUs greater than 1500, so as to prevent fragmentation. For diversion or redirection, PBR-GRE is similar to the PBR-L2TPv3 technique, except that router implementation differences may result in different performance results.

C. Viable Re-Routing Techniques

In the next section, we evaluate some of these diversion and redirection techniques. We do not consider MPLS re-routing in our evaluation. This form of diversion and redirection has the strictest constraint in terms of equipment needed - it can only be applied in a network that uses MPLS technology. However, in an MPLS network, it is unlikely that any re-routing technique other than MPLS would outperform it. We do not consider the eBGP technique since there is little apparent benefit over the iBGP technique and it comes at additional configuration complexity. We also do not consider the VRF based techniques in our evaluation because our testbed cannot adequately model a real VRF scenario. Thus, we evaluate the remaining four combinations of techniques:

- iBGP for diversion and PBR-L2TPv3 for redirection
- iBGP for diversion and PBR-GRE for redirection
- PBR-L2TPv3 for diversion and iBGP for redirection
- PBR-GRE for diversion and iBGP for redirection

In these techniques, a set of tunnels can be set up during preparation to reduce configuration overhead during an attack. If used in diversion, tunnels can be set up from each ingress router to each cleaning center, or vice-versa for redirection. When an attack occurs, PBRs can then be manually inserted or automated through re-configuration scripts. Similarly for de-activation, the PBRs can be removed. In this way, the administration overhead can be kept to a minimum. Similarly, the iBGP announcements can be automated through re-configuration scripts.

V. Performance Results

We now examine the performance of a sample cleaning center architecture, under varying attack loads and varying applications for each of the four combinations of traffic re-routing techniques. We examine them in a limited testbed. The goal of this evaluation is to show that techniques for the necessary re-routing exist and that they are viable. The goal is not to compare them. In fact, the results are comparable between them. The performance metrics that we consider here are the latency response of valid application traffic and the percentage of valid traffic that is dropped.

A. Evaluation Testbed

We evaluate this form of DDoS mitigation using a testbed that we constructed in a laboratory environment shown in Figure 4. The attackers are workstation servers running custom attack code. The generator is a high end server that generates valid traffic toward the victim. The victim is a high end server running a web daemon and a DNS daemon [2]. The monitoring machine measures the application response time of pings, HTTP requests and DNS requests to the victim. It records the average latency reported by the ping command. The average HTTP request latency is obtained from timestamps at the start of a TCP handshake for an HTTP GET and at the end of the session after the transfer is complete. Each HTTP transfer involves 3.73 KB of data [3]. DNS request latency is the time nslookup takes to successfully complete a lookup. A non-response is recorded as a request loss. Some amount of jitter will be introduced from variable operating system delay and network delay. The mitigator is a commercially available inline scrubbing device. The network consists of gigabit-Ethernet and fast-Ethernet links, four Cisco routers and a Foundry router [4].

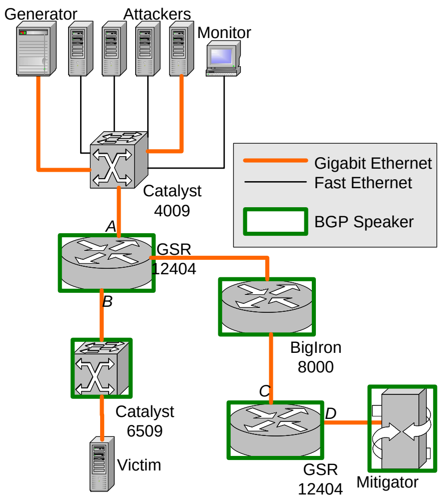

Fig. 4. Evaluation Testbed

For each of the four re-routing scenarios, we use the following set-up. For iBGP diversion, we use the mitigation device to propagate iBGP announcements for the victim address range. For PBR-L2TPv3 diversion, we create a tunnel between port A on the Cisco GSR 12404 connected to the Catalysts and port D on the Cisco GSR 12404 next to the mitigation device. We use PBR rules on the top GSR to force all traffic to the victim address range received on port A to enter the tunnel. A PBR rule on the bottom GSR causes all traffic received on the tunnel to go to the mitigator. For PBR-GRE diversion, we use a similar configuration to create a layer-3 tunnel attached to port A of the top GSR and to port D on the bottom GSR next to the mitigator, with similar PBR rules.

For iBGP redirection, no change is necessary as the Cisco Catalyst 6509 already has the normal path in BGP for reaching the victim through it. For PBR-L2TPv3 redirection, we create a tunnel between port B of the top GSR and port D of the GSR next to the mitigator. PBR rules cause traffic from the mitigator to the victim to be forced through the tunnel on the bottom GSR. For the PBR-GRE redirection, we create a tunnel with the associated PBR rules between port D of the GSR next to the mitigator and the Catalyst 6509. We use the Catalyst in this scenario instead of the top GSR because it avoids having to apply additional PBR rules to force traffic to the victim.

One of the key concerns in designing a cleaning center is the

[2] It is a dual 2 GHz CPU Windows XP SP1 server with 1 GB of RAM running Microsoft IIS 5.0 and BIND-PE 1.2.0.1.

[3] In comparison, the size of the default post set up page of the Apache webserver is 3.85 KB.

[4] The Cisco GSR 12404s are running IOS 12.025S1, the Cisco Catalyst 6509 is running in Hybrid Mode 12.1.13, and the Cisco Catalyst 4009 router is running version 12.1.8. The Foundry BigIron 8000 is running Ironware 7.3.

amount of router configuration overhead that is required. We pick these four re-routing techniques primarily because they are the most straight forward to implement. For that reason, they all have a similar configuration overhead. The number of configuration lines that need to change for iBGP redirection or diversion is linearly dependent on the number of victim prefixes, and would be applied upon detecting an attack. A GRE tunnel takes at least 4 lines of configuration change on each end of the tunnel and for L2TPv3 tunnels, it is 6. Applying a PBR rule requires 2 lines per router and an additional line for every interface that it is applied to. The tunnels can be prepared in advance of an attack, and the PBR rules can be applied to the relevant interface upon detecting an attack. Overall, we believe this overhead is insignificant for these four techniques.

B. Evaluation Methodology

For each of the four re-routing combinations, we evaluate the application response time penalty and loss in nine different scenarios. In all scenarios, there is constant valid traffic from the generator to the victim of 26 Mbps. This consists of 60% HTTP GETs, 10% DNS lookups, 20% FTP traffic, 5% of miscellaneous UDP traffic and 5% of miscellaneous TCP traffic. In the “Normal” scenario, we measure the ICMP ECHO latency, DNS lookup latency and HTTP GET latency 10 times every 60 seconds from the monitor to the victim. We average the latency results across 15 minutes of running time. In the remaining scenarios, we introduce attack traffic from the attackers at varying rates. The attacks are a combination of a UDP flooding attack, a TCP SYN flooding attack and an ICMP flooding attack at 20%, 50% and 30% of attack bandwidth respectively.

In the “15 Mbps Attack” scenario, we introduce 15 Mbps of attack traffic for 30 minutes while still measuring the latency as in the previous scenario. However, the latency tends to vary at the start of the test, and so we only report the average latency once the response latency stabilizes. We also measure the number of requests from the monitor that are lost. In the “15 Mbps Attack Mitigation” scenario, we turn on the re-routing technique and for 15 minutes we measure the latency experienced. Again, we only report the average steady state latency, and this represents the additional delay due to both re-routing and the inline scrubbing device. Similarly, we test “50 Mbps Attack” and “100 Mbps Attack” scenarios.

C. Results

We present the results in Table I. The rows show the impact on the three different kinds of traffic - pings, DNS lookups and HTTP gets. The first column shows the latency during normal circumstances with no attack traffic. The remaining columns are segmented by amount of attack traffic - 15, 50 or 100 Mbps. Within each of these classes, there are four columns. The first two columns show the latency and percentage loss of legitimate requests at the monitor during the attack, without any mitigation. The last two columns show these values after re-routing is enabled and the traffic is scrubbed through the mitigator. The “N/A” values for latency indicate that the victim did not respond to any valid requests. As the tables illustrate, in most cases, the use of the cleaning center reduced valid traffic loss and reduced valid traffic latency during attacks, but not to the pre-attack levels. This is because the diversion, redirection and cleaning process all add latency.

We can make several observations of this data on our evaluation scenario. Firstly, ICMP ECHO packets or pings rarely suffered in terms of loss or latency during the attacks due mainly to attack intensity and type, but performed expectedly worse during mitigation due to the additional distance that the packets had to travel. In our tests, DNS tends to suffer immediately even in low attack conditions as the latency increases from about 3.5 ms to over 20 ms or even becoming unreachable. That is why during mitigation, DNS latencies improved significantly because the additional latency from the redirection and cleaning was more than offset by the reduced server load. HTTP GETs did not suffer as much in our low bandwidth attacks but then became rapidly unresponsive in higher bandwidth attacks. HTTP latency improved more dramatically with mitigation for high bandwidth attacks. These results are similar across all four combinations of re-routing techniques.

Thus, we conclude that cleaning center mitigation is a viable concept for deploying in an ISP. Our results show that during an attack, this technique can dramatically increase the amount of legitimate traffic that is handled and reduce the latency that is experienced by it. However, this latency is higher than the pre-attack levels, due to both re-routing and the cleaning device, as seen by the increases in ICMP delay. For low bandwidth attacks, some benefit can be seen with mitigation, but that benefit may be even smaller when considering wide area latencies. For high bandwidth attacks, mitigation always improved HTTP and DNS response times.

Note that in our attacks, we did not saturate the network connection to the victim. In that case, the cleaning center mitigation will perform even better since a saturated network connection can make the victim server unresponsive from the monitor’s perspective. Also, this attack occurred in a laboratory environment and did not consider wide area latencies in re-routing. This latency penalty will depend on a variety of factors, including the location of the attackers, the location of the victims and the number and locations of the cleaning centers.

VI. Conclusions

We have introduced the concept of regional cleaning centers for DDoS attack mitigation. Under this approach, traffic destined to a victim under a DoS (or DDoS) attack, is routed to a cleaning center for cleaning. After filtering out the malicious packets, the traffic is routed back to the original destination. We described the architecture of a cleaning center, identified its main components and explained the SLA requirements that need to be considered for this new service. We also presented a set of approaches to achieve traffic diversion and redirection which are essential for any implementation of a cleaning center. The availability of certain resources that each approach requires would determine its feasibility in certain environments. Finally, we showed results from a sample cleaning center in which we varied the approach used for both traffic diversion and redirection. The results indicate that cleaning centers can be a viable option for traffic conditioning, provided that its implications in the dynamics of traffic are part of a network-wide traffic engineering process. For future work, we need to investigate and quantify

		15 Mbps Attack				50 Mbps Attack				100 Mbps Attack			
	Normal	Attack	Loss	Mitigation	Loss	Attack	Loss	Mitigation	Loss	Attack	Loss	Mitigation	Loss
iBGP Diversion and PBR-L2TPv3 Redirection													
ICMP	0.32	0.38	0%	0.75	0%	0.32	0%	1.15	0%	0.40	0%	1.10	0%
DNS	3.48	35.00	0%	18.00	0%	20.00	20%	10.05	0%	90.00	10%	12.00	0%
HTTP	3.05	6.20	5%	4.00	0%	N/A	100%	3.50	0%	N/A	100%	6.00	0%
iBGP Diversion and PBR-GRE Redirection													
ICMP	0.32	0.35	0%	1.20	0%	0.35	0%	0.82	0%	0.31	0%	1.00	0%
DNS	3.48	28.60	0%	9.97	0%	20.00	50%	10.03	0%	N/A	100%	10.00	0%
HTTP	3.05	6.00	10%	3.20	0%	N/A	100%	2.50	0%	N/A	100%	5.70	0%
PBR-L2TPv3 Diversion and iBGP Redirection													
ICMP	0.32	0.40	0%	1.10	0%	0.35	5%	1.10	0%	0.50	5%	1.30	0%
DNS	3.48	30.10	0%	9.90	0%	25.00	10%	12.00	0%	N/A	100%	11.00	0%
HTTP	3.05	7.00	10%	3.80	0%	N/A	100%	4.00	0%	N/A	100%	5.50	0%
PBR-GRE Diversion and iBGP Redirection													
ICMP	0.32	0.36	0%	1.10	0%	0.37	5%	0.90	0%	0.40	5%	1.15	0%
DNS	3.48	30.10	0%	10.00	0%	28.50	20%	9.85	0%	N/A	100%	11.00	0%
HTTP	3.05	6.00	5%	3.50	0%	N/A	100%	3.10	0%	N/A	100%	4.00	0%

TABLE I

PERFORMANCE RESULTS (TIME IN MILLISECONDS)

the impact of traffic diversion and redirection on the traffic planning and forecasting process. Although we introduced the concept of cleaning centers for DDoS attack mitigation, there are additional benefits derived from the fact that it can be utilized in a variety of other applications/services. Such applications include traffic logging, monitoring, measurement, and analysis for traffic engineering or auditing purposes.

ACKNOWLEDGMENTS

The authors would like to thank Scott Alcaide for the initial discussions and work related to the various diversion techniques. We are also indebted to George Apostolopoulos, Christos Papadopoulos, Clay Shields, and Nina Taft for detailed feedback on earlier versions of this paper.

REFERENCES

[1] L. Garber, “Denial-of-service attacks rip the Internet.” Computer, 2000.

[2] C. Shields, “What do we mean by network denial of service?,” in *Proceedings of the IEEE Workshop on Information Assurance and Security*, (West Point, NY), June 2002.

[3] S. Staniford, V. Paxson, and N. Weaver, “How to 0wn the Internet in your spare time,” in *11th USENIX Security Symposium*, 2002.

[4] A. Keromytis, V. Misra, and D. Rubenstein, “SOS: Secure overlay services,” in *SIGCOMM*, ACM, 2002.

[5] D. G. Andersen, “Mayday: Distributed filtering for Internet services,” in *4th Usenix Symposium on Internet Technologies and Systems, Seattle, Washington*, March 2003.

[6] K. Park and H. Lee, “On the effectiveness of Route-Based packet filtering for distributed DoS attack prevention in Power-Law internets,” in *Proc. ACM SIGCOMM*, August 2001.

[7] B. R. Greene, C. L. Morrow, and B. W. Gemberling, “ISP security - Real World Techniques.” NANOG-23 Tutorial, October 2001.

[8] P. Ferguson, “Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing,” tech. rep., Internet RFC 2827, May 2000.

[9] Cisco, “Unicast reverse path forwarding (uRPF).” http://www.cisco.com.

[10] A. K. Ghosh, J. Wanken, and F. Charron, “Detecting anomalous and unknown intrusions against programs,” in *Annual Computer Security Application Conference (ACSAC’98)*, pp. 259–267, IEEE CS Press, 1998. Los Alamitos, California.

[11] M. Roesch, “Snort – lightweight intrusion detection for networks,” in *Usenix Lisa ’99*, Usenix Association, 1999. Berkeley, California.

[12] V. Paxson, “Bro: A system for detecting network intruders in real-time,” in *Seventh Usenix Security Symposium*, Usenix Association, 1998. Berkeley, California.

[13] S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, “Practical network support for IP traceback,” in *SIGCOMM*, pp. 295–306, 2000.

[14] C. Morrow and B. Gemberling, “Backscatter traceback.” http://www.secsup.org/Tracking/.

[15] J. Ioannidis and S. M. Bellovin, “Implementing pushback: Router-based defense against DDoS attacks,” in *Proceedings of Network and Distributed System Security Symposium*, February 2002.

[16] R. Stone, “CenterTrack: An IP Overlay Network for Tracking DoS Floods,” in *Proceedings of the 9th USENIX Security Symposium*, (Denver, CO), August 2000.

[17] Y. Rekhter and T. Li, “A border gateway protocol 4 (BGP-4),” RFC 1771, March 1995.

[18] G. Iannaccone, S. Bhattacharyya, N. Taft, and C. Diot, “Always-on monitoring of IP backbones: Requirements and design challenges,” Sprint ATL Research Report RR03-ATL-071821, Sprint ATL, 2003.

[19] D. Oran, “OSI IS-IS intra-domain routing protocol,” RFC 1142, IETF, February 1990.

[20] J. Moy, “OSPF version 2,” RFC 1583, IETF, March 1994.

[21] C. Partridge, T. Mendez, and W. Milliken, “Host anycasting service,” tech. rep., Internet RFC 1546, November 1993.

[22] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol label switching architecture,” RFC 3031, January 2001.

[23] E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” RFC 2547, IETF, March 1999.

[24] Cisco, “Policy-based routing.” White Paper, 1996.

[25] J. Lau, M. Townsley, and I. Goyret, “Layer two tunneling protocol (version 3),” tech. rep., Internet Draft, July 2003. draft-ietf-l2tpext-l2tp-base-09.

[26] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, “Generic routing encapsulation (GRE),” RFC 2784, March 2000.

[27] Cisco, “Why can’t I browse the Internet when using a GRE tunnel?,” warp support document, 2003.