AFRL-RI-RS-TR-2021-090

PLANNING FOR ANYCAST AS ANTI-DDOS (PAADDOS)

UNIVERSITY OF SOUTHERN CALIFORNIA

MAY 2021

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2021-090 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
WALTER S. KARAS
Work Unit Manager

/ S /
JAMES S. PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2021	FINAL TECHNICAL REPORT	NOV 2018 - DEC 2020

4. TITLE AND SUBTITLE

PLANNING FOR ANYCAST AS ANTI-DDOS (PAADDOS)

5a. CONTRACT NUMBER
FA8750-19-2-0003

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
69220K

6. AUTHOR(S)

John Heidemann (USC/ISI)

5d. PROJECT NUMBER
PAAD

5e. TASK NUMBER
DO

5f. WORK UNIT NUMBER
S1

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of Southern California
Information Sciences Institute
4676 Admiralty Way, Ste. 1001
Marina del Rey CA 90292

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2021-090

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This final report summarizes the objectives for the PAADDoS project and the technical progress made against those objectives. The PAADDoS project's goal is to defend against large-scale Distributed Denial-of-Service (DDoS) attacks by making anycast-based capacity more effective than it is today. Anycast use Internet routing to associate users with geographically close sites of a replicated service. PAADDoS helps anycast manage DDoS attacks by developing tools and methods to (1) map catchments, (2) change catchments in response to DDoS, (3) estimate attack size.

15. SUBJECT TERMS

Anycast, DNS, distributed denial-of-service attacks, DDoS defense

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**WALTER S. KARAS**
U	U	U	UU	33	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SUMMARY

This final report summarizes the objectives for the PAADDoS project and the technical progress made against those objectives. The PAADDoS project's goal is to defend against large-scale Distributed Denial-of-Service (DDoS) attacks by making anycast-based capacity more effective than it is today.

Anycast use Internet routing to associate users with geographically close sites of a replicated service. PAADDoS helps anycast manage DDoS attacks by developing tools and methods to (1) map catchments,

(2) change catchments in response to DDoS, (3) estimate attack size. Each of these key results are described in Section 4.1. Section 4.2 provides a summary of activities over the course of the project, including technical accomplishments, deliverables, publications, and meetings. Finally, Section 5 summarizes the project's key accomplishments, technology transfer activities, and recommendations.

2.0 INTRODUCTION

Performer: University of Southern California
Project Title: Plannning for Anycast as Anti-DDoS (PAADDoS)
Agreement number: FA8750-19-2-0003
Period of Performance: 2018-10-01 to 2020-10-31, with a no-cost extension to 2020-12-31
Estimated Total Award Value: $248k

2.1 PI of Record and Programmatic/Technical Reporter

John Heidemann, office telephone: +1 (310) 448-8708, e-mail address: johnh@isi.edu

2.2 Administrative Contact

Jeanine Yamazaki, office telephone +1 (310) 448-8228, e-mail address: yamazaki@isi.edu

2.3 Financial Data Reporter

Joe Kemp, office telephone: +1 (310) 448-9171, e-mail address: kemp@isi.edu

2.4 Recipient Monitor

None

2.5 Sub Recipient

None, although there is a parallel project supervised by NWO at the University of Twente, with Aiko Pras as PI.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Research Objectives

Huge Distributed Denial-of-Service (DDoS) attacks such as the fall 2016 Mirai-botnet attacks open a new phase in the DDoS threat. A decade of research has improved end-device security and reduced some forms of DDoS attack (for example, address spoofing and amplification prevention). But *millions of embedded, Internet-of-Things (IoT) devices are deployed to the Internet each day*, Mirai shows they can be weaponized—the threat of multi-thousand-node botnets making legitimate network requests represents the ultimate limit of DDoS. With ever new devices that are too cheap to secure, the threat cannot be prevented, and their ability to make widely distributed but *fully legitimate* DNS queries means they cannot be easily filtered.

Widespread anycast is necessary to provide sufficient capacity while being cost-effective. Although anycast is widely used in DNS and CDNs today, existing tools to plan and manage anycast are limited, and no tools exist to reconfigure anycast when under attack.

This proposal will address this challenge, countering the IoT DDoS threat by making anycast-based capacity effective. Meeting this challenge addresses the *Distributed Denial-of-Service Defense* TTA of the joint DHS S&T/CSD-Netherlands solicitation. We will provide four new capabilities: (1) tools to *map anycast catchments* and baseline load, (2) methods to *plan changes* and their effects on catchments, and (3) tools to *estimate attack load* and assist anycast reconfiguration curing an attack. *Raw capacity* is required to meet the most serious DDoS threats, that *anycast* is required to get that capacity cost- effectively, and that *our tools are essential to make anycast agile under stress*. Anycast today is under- deployed before attacks and less effective because of its inflexibility during attacks.

These capabilities will be possible through our unique insights into the problem: Our approach, Verfploeter, is the first to employ *active probing for catchment mapping*, identifying which anycast site is assigned to millions of end-user networks. We combine this information with historical traffic information to map load, and will use *active probing and modeling to provide complementary methods to plan how this load shifts* as anycast changes. The result will be methods that can be used for both pre- deployment planning and response during attacks, assisted by *attack-rate estimates that use traffic trends for calibration* even when attacks exceed network capacity. Our approaches will complement existing methods of filtering to provide network services that can manage attacks to multiple terabits per second.

This proposal builds on two years of collaboration and joint work in the area of DNS and anycast between USC/ISI and the University of Twente.

3.2 Public Problem Description

3.2.1 Public Research Goals/Contribution

The PAADDoS project's goal was to defend against large-scale Distributed Denial-of-Service (DDoS) attacks by making anycast-based capacity more effective than it is today. Anycast use Internet routing to associate users with geographically close sites of a replicated service. During

DDoS, anycast sites can provide capacity to absorb an attack, and they can be used to isolate the attack to part of the network.

PAADDoS worked toward our goal of improving anycast use during DDoS by (1) developing tools to *map anycast catchments* and baseline load, (2) develop methods to *plan changes* and their effects on catchments, and (3) develop tools to *estimate attack load* and assist anycast reconfiguration during an attack.

3.2.2 Expected Impact

We expect the innovations developed in the PAADDOS project to improve service resilience in the face of DDoS attacks. Our tools will improve *anycast agility* during an attack, allowing capacity to be used effectively.

3.3 Technical Approach

3.3.1 Detailed Description of Public Technical Approach: Methods and Procedures

Ultimately, the main defense against huge amounts of legitimate traffic is capacity and anycast. One cannot grow an individual data center arbitrarily—the cost of very large links, with matching firewalls, load balancers, and back end computers grows exponentially as capacity exceeds 100 Gb/s today, and the highest-end performance will always come at a premium. Moreover, when the attack exceeds capacity, anycast can split the service into pieces (by catchment), allowing some to continue to offer service even if others are overwhelmed. We therefore believe that anycast is the only cost-effective method to reach DDoS-tolerant capacities, where many moderate-bitrate sites (10 to 100 Gb/s) cooperate to provide aggregate capacities in the multi-Tb/s range.

Our approach leverages the observation that capacity and anycast are the only way to counter DDoS attacks performed by huge botnets. That cost-effective capacity requires anycast, and managing anycast under stress and choices about shifting traffic or allowing partially degraded service require better tools so the defender can make the *best* choice among alternatives. This project explored three specific tools to help assist defenders in countering this threat.

First, we explored new tools to map anycast catchments and estimate load. Anycast *catchments* specify which networks reach which anycast sites, and they are determined by the interaction of BGP policies around the Internet. In preliminary work we presented *Verfploeter*, a tool that allows mapping of anycast catchments with much finer precision (to /24 prefixes) than before, supporting *accurate estimation of current load* and *prediction of the impact of a DDoS attack*.

Second, we explored new tools to support understanding how changes will affect anycast catchments, to assist operators as they alter routing before and during an attack. Service operators have the option to influence routing at their anycast sites, steering traffic towards or away from specific sites. The tools for such control are limited, and they will interact with routing policies in their upstream ISPs, and their upstream providers as well. In addition, operators sometimes have the option to deploy new sites, either bringing new, pre-deployed or latent sites on-line, or deploying emergency sites on borrowed hardware or services. In both

cases, the operator would like to plan how such actions will affect their service, rather than making changes blindly.
Third, we developed tools to estimate offered load during an attack. Of course service operators have tools to monitor their networks, but such tools often saturate during DoS attacks. Network monitoring tools know how to estimate utilization only up to 100%, while attacks may drive networks to 150% or 1000% of normal traffic. We believe new tools can *estimate* approximate attack load, thereby providing critical advice to distinguish between the two outcomes of traffic engineering: will shifting traffic absorb the attack over more sites with *enough* capacity, or will it instead spread the damage to *more legitimate users* with additional sites becoming overloaded.

3.3.2 Detailed Description of Approach: Assumptions

Our assumptions are that the defender operates an IP anycast system, with multiple, physically distributed sites. At each site, the defender should have the ability to control routing.

Although we design our system for DNS, our approaches are applicable to other anycast networks such as some CDNs.

We do *not* assume the defender can use DNS to redirect traffic. Although CDN operators often use DNS to redirect traffic to specific locations, a DNS operator cannot easily change the DNS bindings for their zone, and each Root DNS operators necessarily run on a single IP address for IPv4 and another for IPv6. Changing a Root DNS is an extended process usually requiring more than 12 months.

3.3.3 Comparison with Current Technology

There have been several prior approaches to measure anycast catchment using a variety of techniques.

Use of Open Resolvers: Early work used Open DNS Resolvers in combination with PlanetLab and Netalyzr to map catchments of anycast services [Fan13a]. While Open Resolvers provided a broad view at the time of their study (300k VPs), they are being steadily shut down out of concerns about their use in DNS amplification attacks [Mauch13a]. While open resolvers offered a very large set of vantage points, they are fewer than the method we propose that uses ping-responsive networks. (A direct comparison is potential future work.)

Measurement Platforms: The most common method of assessing anycast is to use public or private measurement platforms that offer physical or passive VPs around the Internet. RIPE Atlas and PlanetLab are both openly available and widely distributed, and a number of commercial platforms are also available. Systems we are aware of range from hundreds to around 10k VPs.

Several studies, both by others and us, have used measurement platforms to study anycast [Fan13a, Madory10a, Calder15a, Cicalese15a, Bellis15a, Moura16b, Schmidt17a, Aben17a]. As pre-deployed measurement platforms these systems are available and can measure anycast services externally (without requiring support from the service operator). The main weaknesses of these systems are that they are slow and expensive to grow, and deployment is often skewed

relative to the population of Internet users. This skew has been noted in many prior studies and was recently studied explicitly [Bajpai15a].

Client-side measurements: Recent work examined the Microsoft Bing CDN [Calder15a], using both log analysis (see below) and active client-side measurements. Their client-side analysis measures performance using JavaScript injected into search results of a small fraction of Bing users. Client-side measurements can get very broad results (like Verfploeter), but are not possible for all services. DNS and other non-web services do not support client-side modifications, and may also be difficult for websites hosted by multiple parties.

Traffic and Log Analysis: Anycast operators have always been able to assess current anycast performance by analyzing their own traffic and server logs. Recent work examined a variety of CDNs [Calder15a, Giordano16a]. As the service operator, log analysis requires no external measurements and can cover the entire service. While important, analysis of existing services can only study the *current* deployment—it requires active use by a large number of users and cannot directly support pre- deployment planning. Second, log files may be unavailable due to privacy concerns, cost of storage or retrieval, or concerns about performance impact on operational services. We use logs when available, but do not require them.

Performance Analysis of DNS Services: There have been a number of analysis of root DNS service, both pre-anycast [Fomenkov01a] and with anycast for latency [Liang13a, Fan13a, Cicalese15a, Bellis15a, Schmidt17a] and DDoS [Moura16b].

To the best of our knowledge, our paper is the first to present this ICMP-based anycast catchment determination approach. Further, we do not know of any larger scale catchment measurement with open datasets against a real-world anycast deployment. Ultimately, the main defense against huge amounts of legitimate traffic is capacity and anycast. One cannot grow an individual data center arbitrarily—the cost of very large links, with matching firewalls, load balancers, and back end computers grows exponentially as capacity exceeds 100 Gb/s today, and the highest-end performance will always come at a premium. Moreover, when the attack exceeds capacity, anycast can split the service into pieces (by catchment), allowing some to continue to offer service even if others are overwhelmed. We therefore believe that anycast is the only cost-effective method to reach DDoS-tolerant capacities, where many moderate-bitrate sites (10 to 100 Gb/s) cooperate to provide aggregate capacities in the multi-Tb/s range.

3.4 Schedule and Milestones.

3.4.1 Schedule Graphic

Deliverables in the graphic are keyed to items in the next section.

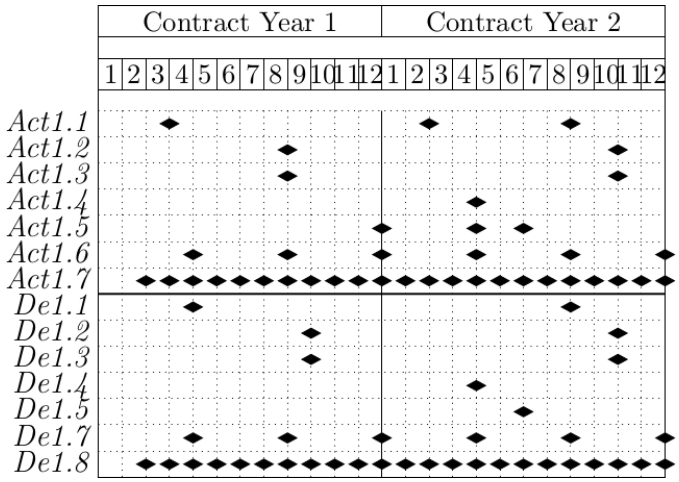

Figure 1 Activities Over Time

3.4.2 Detailed Individual Task Descriptions

3.4.2.1 Task 1: Anti-DDoS Techniques

Overall objective is to develop new techniques to assist anycast systems in surviving DDoS attacks.

3.4.2.1.1 Act 1.1

Provide and evaluate an enhanced version of the Verfploeter tool for anycast catchment mapping: (a) provide basic version of Verfploeter with catchment mapping and load estimation (S+3m), (b) evaluate measurement frequency (S+14m), (c) demonstrate Verfploeter on test network (S+9m), (d) release updated version based on what was learned (S+20m)

3.4.2.1.2 Act 1.2

(a) Provide basic measurement-based tool for what-if evaluation on test prefix (S+8m), (b) provide updated tool based on experience (S+22m)

3.4.2.1.3 Act 1.3

(a) Demonstrate basic modeling of anycast catchments (S+8m), (b) compare modeling and experiments (S+22m)

3.4.2.1.4 Act 1.4

Provide library of DDoS attacks to test model (S+16)

3.4.2.1.5 Act 1.5

(a) Demonstrate approach to estimate attack size (S+12m), (b) provide tool to estimate attack size (s+16m), (c) provide tool to assist in attack response (S+18m)

3.4.2.1.6 Act 1.6

Participate in PI meetings

3.4.2.1.7 Act 1.7

Provide project plan, technical and financial reports

3.5 Deliverables Description

Deliverable dates are given as start of contract + N months (S+Nm).

3.5.1 Deliverable 1.1

Verfploeter tool to evaluate anycast catchments (a) basic release (S+4m), (b) updated release (S+20m)

3.5.2 Deliverable 1.2

What-if measurement tool (a) basic release (S+9m), (b) updated release (S+22m)

3.5.3 Deliverable 1.3

Modeling of anycast catchments and load (a) basic release (S+9m), (b) updated release (S+22m)

3.5.4 Deliverable 1.4

DDoS attack models (S+16m)

3.5.5 Deliverable 1.5

Attack response tool, release (S+18m)

3.5.6 Deliverable 1.6

Provide technical status reports (S+4m, continuing)

3.5.7 Deliverable 1.7

Provide financial status reports (S+1m, continuing)
Deliverables will be provided by USC/ISI by contract end-date.

3.6 Technology Transition and Technology Transfer Targets and Plans

The primary outcome of this project was to develop new software tools, coupled with peer-reviewed research papers that demonstrate their capabilities and effectiveness. We have made available papers, reports, and the software we developed through our website.

We demonstrated the utility of our approach through pilot deployments with at two operational partners: B-Root and SIDN. We have a long history of collaboration with several operational web services: we work closely with B-Root at USC. Both U. Twente and USC have collaborated with SIDN Labs, the research branch of SIDN, the national registrar for the Netherlands. U. Twente also works closely with RIPE, the European Regional Registry based in Amsterdam and also operators of K-Root, as well as with SURFnet the Dutch National Research and Education Network (NREN), which operates several DNS services.

We also published the results of our work in peer-reviewed conferences and journals and public technical reports. Public dissemination of the ideas is an important path to see them used in commercial companies, complementing direct distribution of the tools (code) and datasets.

4.0 RESULTS AND DISCUSSION

4.1 Key Results

PAADDoS made advances in anycast mapping, planning responses to DDoS, and estimating attack load. A primary description of these results are in the technical report "Anycast Agility: Adaptive Routing to Manage DDoS" [Rizvi20a]. We summarize each of these key results below.

4.1.1 Mapping Anycast Catchments

B-Root, one of the 13 root DNS servers, deployed three new sites in January 2020, doubling its footprint and adding its first sites in Asia and Europe. How did this growth lower latency to users? We looked at B- Root deployment to answer this question.

To do find anycast catchments, we use Verfploeter to probe over 6 million IPv4 /24 prefixes (or blocks) around the world. Each reply from these blocks shows which site it selects and shows that it is part of that site's catchment.

We visualize anycast catchments on a world map with verfploeter_plotter tool, developed as part of PAADDoS. This tool maps all IP addresses to a latitude/longitude grid and counting how many prefixes in each grid cell go to each site. We show a pie chart in each grid cell, with pie slices showing the fraction of traffic to each site, and pie size showing how many prefixes are in that cell.

B-root added three new sites in January 2020. We measured them with a test prefix since late 2019: Singapore (SIN): 2019-12-20
Dulles (IAD): 2019-12-31
Amsterdam (AMS): 2020-01-03
These sites were added to B's existing 3 sites: Los Angeles (LAX); Arica, Chile (ARI); and Miami (MIA).

4.1.1.1 Before the New Sites

Before adding three new sites, LAX site is more visible than the others.

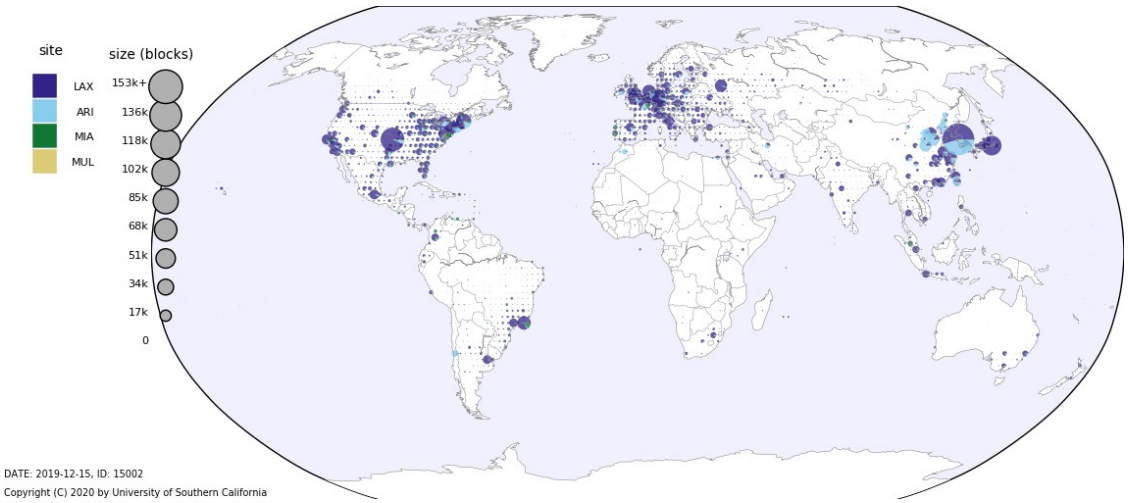

Figure 2 B-Root catchments, before adding additional sites.

4.1.1.2 After Adding Singapore (SIN)

After adding Singapore (SIN, the pink color), most East Asian traffic goes there (see Korea and Japan, for example).

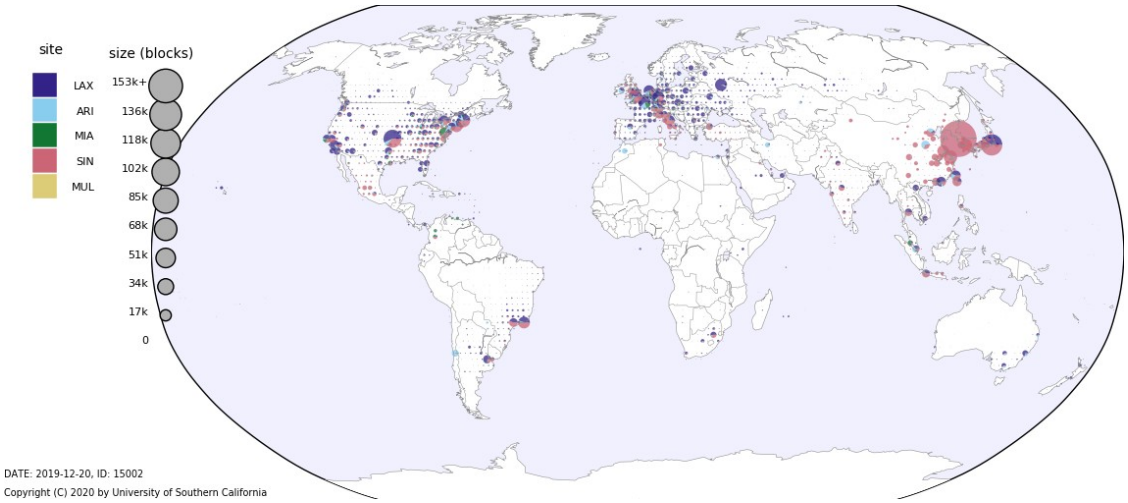

Figure 3 B-Root catchments after adding a fourth site in Singapore (SIN).

4.1.1.3 After Adding Washington, DC (IAD)

The Washington site (IAD, dark red) attracts a significant portion of traffic from the US and Europe.

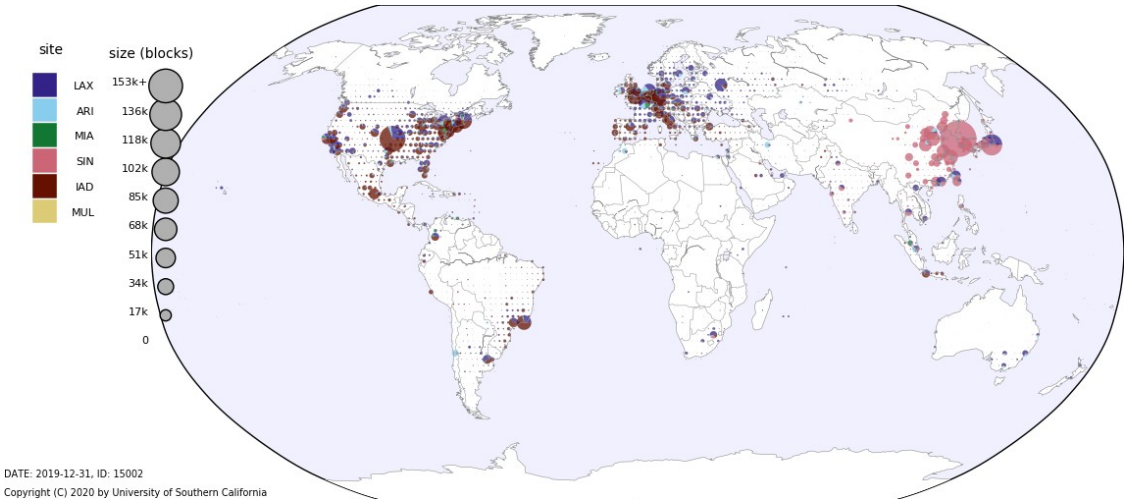

Figure 4 B-Root catchments, after adding a fifth site at Washington, DC (IAD)

4.1.1.4 After Adding Amsterdam (AMS)

The new site in Amsterdam (AMS, the yellow-green color) captures most European traffic. Overall, these maps from the verfploeter_plotter tool developed as part of PAADDoS, help B-Root understand the results of new deployments.

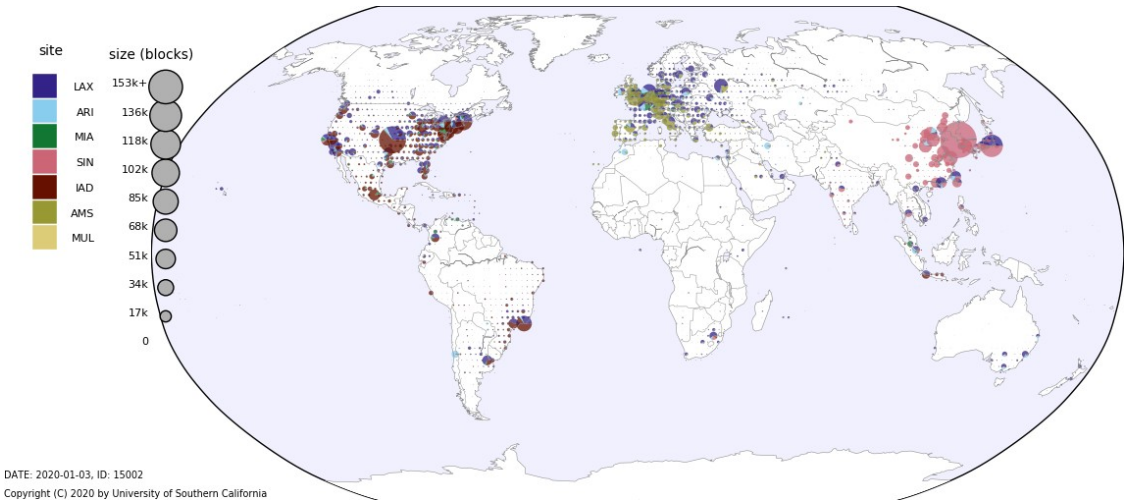

Figure 5 B-Root catchments, after adding a sixth site in Amsterdam (AMS)

4.1.2 Planning for DDoS Response

During the attack we plan to manipulate routing to respond to traffic. But making informed choices about routing changes requires that we have some idea of what effect a change will have. We therefore *map* our anycast catchments and how they change in response to routing changes ahead of any attack.

When mapping catchments, we determine which networks are associated with which anycast sites. We use Verfploeter to find the catchments of the anycast clients using *active probing*. Verfploeter uses a target hitlist of IPs, and probe them with ICMP ECHO request. ICMP REPLY from each target network ends up in its catchment site making the network to anycast site mapping. An alternative is to remember which customers are seen at each site over time or to observe from distributed vantage points such as RIPE Atlas .

Mapping should consider not only the current catchments but also *potential* shifts we might make during the attack. This full mapping is easy to do with Verfploeter, which can be continuously running in an adjacent BGP prefix to map the possible shifts. This mapping process is important to anticipate how traffic may be shifted. In our technical report we show later that BGP control is limited by the granularity of routing policy and by the deployment of the anycast sites.

The actual attack traffic may distort anycast—if the attackers are concentrated in a few networks, routing changes may not spread them out. Even then, mapping helps anticipate how legitimate traffic will shift.

Based on our understanding of prepending and communities, we can now build a playbook of possible traffic configurations for an anycast network.

The table below on the left shows a sample playbook with selected configurations. Operators will be aware of the baseline, and when the site is under attack, if they wish to shift a site to a different balance they can read it off from the table. Of course, if attackers are concentrated on certain locations, traffic may not shift exactly as predicted, but this table is a starting point. Finally, this table also suggests *where traffic ends up* after a reconfiguration. The consequences of operator's actions on other sites are as important as reducing the load on one site.

Routing Policy	Traffic to Site (%) AMS	BOS	CNF
(a) 6peers, 12peers	~5	~35	~55
(b) Route-server	15	35	55
(c) All-IXP-Peers	15	35	45
(d) 3xPrepend AMS	15	35	45
(e) 2xPrepend AMS	25	35	45
(f) 1xPrepend AMS	35	25	35
(g) -3xPrepend BOS	25	65	5
(h) -2xPrepend BOS	35	65	5
(i) -1xPrepend BOS	45	35	5
(j) -3xPrepend CNF	25	15	65
(k) -2xPrepend CNF	35	5	55
(l) -1xPrepend CNF	45	5	45
(m)Transit-1	45	25	35
(n) Transit-2	55	15	25
(o) Baseline	65	15	15
(p) 1,2xPrepend BOS	65	5	25
(q) 3xPrepend BOS	75	5	25
(r) 1xPrepend CNF	85	5	5
(s) 2,3xPrepend CNF	85	15	5
(t) -1,-2,-3xPrepend AMS	85	5	5

Figure 6 Routing Configurations for a three site canycast network

Traffic to Site (%)	AMS	BOS	CNF
0-10	a	k, l, p, q, r, t	g, h, i, r, s, t
10-20	b, c, d	j, n, o, s	o
20-30	e, g, j	f, m	n, p, q
30-40	f, h, k	a, b, c, d, e, i	f, m
40-50	i, l, m	–	c, d, e, l
50-60	n	–	a, b, k
60-70	o, p	g, h	j
70-80	q	–	–
80-90	r, s, t	–	–
90-100	–	–	–
Traffic options	9	5	7

Figure 7 Which combinations achieve a particular target traffic level at each site

Figure 6 shows different routing configurations for a three-site anycast network (AMS, BOS, and CNF in Amsterdam, Boston, and Brazil) . Green or red shading and the percent show the fraction of traffic going to each site.

Figure 7 helps us to quantify the "flexibility" that traffic engineering allows us in this anycast deployment. If we divide the traffic mix into 10% bins, we see that AMS has 9 options, while CNF has 7, and BOS has only 5. Because AMS and CNF mostly exchange traffic within them after a BGP change, and because BOS is less well connected, no configuration with three sites allows BOS to take traffic within 40-60% range.

4.1.3 Estimating True Attack size

Estimating the offered load to each site is an important first step in DDoS defense to allow us to select our defense strategy (spread traffic or absorb, as described next in). (By "offered load", we mean all the traffic sent to the site, before any loss due to DDoS-driven congestion. Ideally the site would handle all this traffic.)

Here we describe *how* we estimate site traffic, and show one testbed experiment that confirms accuracy. In our paper [Rizvi20a] we provide a more complete evaluation and show how it is used to defend against an attack.

Challenge and idea: Offered load is the combination of legitimate traffic and, during an attack, attack traffic that is sent to a site. The main consequence of a DDoS attack is the exhausted resources, and during an attack, the server and its access networks are overwhelmed. As a result, direct measurements at the server detect only *received* traffic. During an attack, received traffic is constrained by the access link and some offered traffic will be lost one or more hops upstream, before we can observe it. Our insight is that we can *directly* infer loss from *examination of end-to-end, known good traffic that is received*, and from loss we can estimate offered load to site.

Approach: We estimate site offered load by measuring the fraction of known good traffic that arrives at the service. We next describe each of these sub-problems.

We want to observe loss of legitimate traffic. Unfortunately, there is no general way to determine the current rate of legitimate traffic—traffic rates constantly change, sometimes unpredictably. Moreover, sophisticated attackers make attack traffic look just like good traffic, making the traffic rate impossible to measure when it is most needed.

We therefore use *subset of known good traffic* to represent all legitimate traffic. For DNS, RIPE Atlas provides a regular source of known-good traffic, sent from many places, with out-of-band reporting. We assume that most commercial services (in addition to DNS) have similar kinds of regular monitoring traffic.

We want offered load, or *Toffered*. We know the observed traffic rate *Tobserved*—it is the access link bitrate, or it can be measured at the access link. We know that α * *Toffered*= *Tobserved*, where α is the accept fraction (the traffic that is not dropped).

To determine α, we observe that known good traffic has the same loss on incoming links as does other good traffic and attack traffic. We know that RIPE Atlas sends measurement traffic at a known, constant rate *Tknown*, so α * *Tknown,offered* = *Tknown,observed*. Solving for α and substituting back gives us: *Toffered* = *Tobserved* * *Tknown,offered* / *Tknown,observed*. We next validate our model with experiments in a testbed. DETERLab is a configurable testbed that enable isolation in a controlled network .

Here we use unequal legitimate traffic, with L_1 of 80 Mb/s and L_2 of 20 Mb/s, so changes to attack traffic on L_1 have greater impact on our estimate. When loss is the same on both links (50% loss with A_1 = 120 Mb/s and A_2 = 180 Mb/s), estimation of site offered load should be accurate. shows this case in the testbed; we slightly underestimate.

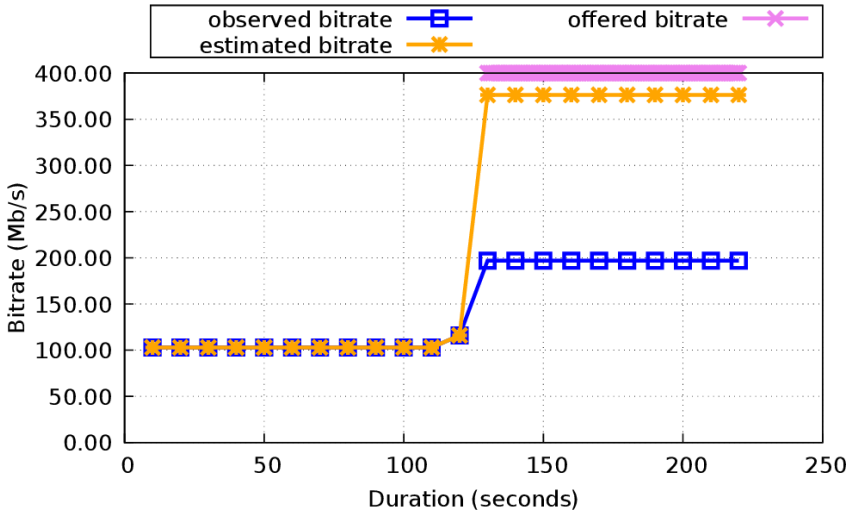

Figure 8 DETERlab experiments to evaluate attack size estimation, from [Rizvi20a, Figure 3].

4.2 Project Activities

4.2.1 Progress Towards Planned Objectives

All project objectives were completed over the course of the project. Details about when objectives are listed below and described in detail in Section 4.2.2 marked [STx].

4.2.1.1 Task 1

Anti-DDoS Techniques: Overall objective is to develop new techniques to assist anycast systems in surviving DDoS attacks.

4.2.1.1.1 Act 1.1

Provide and evaluate an enhanced version of the Verfploeter tool for anycast catchment mapping: (a) provide basic version of Verfploeter with catchment mapping and load estimation (S+3m), (b) evaluate measurement frequency (S+14m), (c) demonstrate verfploeter on test network (S+9m), (d) release updated version based on what was learned (S+20m). *Act1.1 goal (a) completed in 2019 with the initial release of Verfploeter tools at https://ant.isi.edu/software/verfploeter/. Act1.1 goal (b) completed by 2019q3 with evaluation of Verfploeter over B-Root's test prefix. Act1.1 goal (c) completed 2020-02- 25 using B-Root's new sites. Act1.1 goal (d) completed 2020-03 with improved hitlist definition.*

4.2.1.1.2 Act 1.2

(a) Provide basic measurement-based tool for what-if evaluation on test prefix (S+8m), (b) provide updated tool based on experience (S+22m). *Act1.2 goal (a) is underway as of 2019q3,*

and we expect to release public results by 2020q1. Completed 2020-06 with Verfploeter (described above) and description of playbook generation in technical paper "Anycast Agility: Adaptive Routing to Manage DDoS".

4.2.1.1.3 Act 1.3

(a) Demonstrate basic modeling of anycast catchments (S+8m), (b) compare modeling and experiments (S+22m). *Act1.3 goal (a) is described in the 2020q1 quarterly report. Act.1.3 goal (a) completed 2020-02-25 with modeling of B-Root.*

4.2.1.1.4 Act 1.4

Provide library of DDoS attacks to test model (S+16) . *Act1.4 completed early in 2019q3 with release of 5 B-Root-anomaly datasets at https://ant.isi.edu/datasets/ and https://impactcybertrust.org.*

4.2.1.1.5 Act 1.5

(a) Demonstrate approach to estimate attack size (S+12m), (b) provide tool to estimate attack size (s+16m), (c) provide tool to assist in attack response (S+18m). *Act1.5 goal (a) and (b) completed 2020- 02 with attack size estimation tool. The tool is released (c) at https://ant.isi.edu/software/.*

4.2.1.1.6 Act 1.6

Participate in PI meetings. *Act1.6 was completed with PI meetings in 2019-01-08 at the DHs cyber showcase, a site visit 2019-07-22, and a PI meeting 2019-10-24.*

4.2.1.1.7 Act 1.7

Provide project plan, technical and financial reports. *Initial report provided 2018-12 with project plan. Financial reports were provided monthly. Technical reports provided on calendar quarters.*

4.2.2 Technical Accomplishments Over The Project

A detailed, chronological list of technical accomplishments over the project are in the last quarterly technical report. [AccNN] references in this document point to those events.

4.2.3 Scientific Highlights

[Pre6] On 2019-10-15, Giovane Moura presented the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at RIPE-79 in Rotterdam, The Netherlands. This peer-reviewed paper represents technology transfer to the community from PAADDoS, and it shows collaboration between USC, U. Twente, and SIDN Labs in the US and Netherlands.

[SciHi1] On 2019-12-18 John Heidemann attended and participated in the PhD defense of

Wouter de Vries at U. Twente (Aiko Pras, PhD advisor). This PhD defense is a concrete example scientific exchange between the US and Netherlands.

[Act1.1c] [Act1.3a] On 2020-02-25, ASM Rizvi and John Heidemann posted "B-Root's new sites reduce latency" at https://ant.isi.edu/blog/?p=1425, using Verfploeter_plotter to visualize how the deployment of three new sites for B-Root (in Singapore, Washington, DC, and Amsterdam) reduced B-Root latency. This deployment at B-Root was influenced by PAADDOS-provided software, a concrete example of technology transfer to operations. [Pub5] On 2020-06-24, we released the paper by ASM Rizvi, Joao Ceron, Leandro Bertholdo, and John Heidemann: "Anycast Agility: Adaptive Routing to Manage DDoS". Technical Report N. arxiv:2006.14058v1, arXiv, June, 2020. <https://arxiv.org/2006.14058>.

4.2.4 Deliverables Over the Project

For progress against deliverables over the course of the project, please see all items listed in Section 4.2.2 marked [Dx]. All deliverables were completed in the project's period-of-performance.

4.2.4.1 Deliverable 1.1

Verfploeter tool to evaluate anycast catchments (a) basic release (S+4m), (b) updated release (S+20m) [Soft1]*Deliverable (a) completed in 2019 with the initial release of Verfploeter tools at https://ant.isi.edu/software/verfploeter/. (b) Completed 2020-03 with updated Verfploeter Hitlist.*

4.2.4.2 Deliverable 1.2

What-if measurement tool (a) basic release (S+9m) (b) updated release (S+22m). [Soft2] *Deliverable (a) partially completed 2019-10-24 with release of Verfploeter/Plotter. Completed 2020-06 with combination of Verfploeter and description of playbook construction method.*

4.2.4.3 Deliverable 1.3

Modeling of anycast catchments and load (a) basic release (S+9m), (b) updated release (S+22m). [Soft2] *Deliverable (a) completed 2019-10-24 with release of Verfploeter/Plotter.*

4.2.4.4 Deliverable 1.4

DDoS attack models (S+16m). *Completed; in 2019q1 we released several DDoS datasets derived from B-Root traces.*

4.2.4.5 Deliverable 1.5

Attack response tool, release (S+18m). *Completed 2020-02 and 2020-09 with release of qname and response filters, and with Verfploeter and playbook.*

4.2.4.6 Deliverable 1.6

Provide technical status reports (S+4m, continuing). *Completed; provided initial project information and description is provided with this report as of 2018-12 and quarterly status reports through project lifetime.*

4.2.4.7 Deliverable 1.7

Provide financial status reports (S+1m, continuing) *Completed; provided on a monthly basis from project beginning.*

4.2.5 Results and Highlights of Interest to the General Public

[Pre6] On 2020-02-25, the PAADDoS project reported about "B-Root's new sites reduce latency" at https://ant.isi.edu/blog/?p=1425. B-Root is one of the 13 DNS services providing the DNS "root" (the service that helps locate .com, .us, and other top-level domains). B-Root used software developed by the PAADDOS project to visualize how the deployment of three new sites for B-Root (in Singapore, Washington, DC, and Amsterdam) reduced B-Root latency. The end result of this deployment is faster access to the DNS for all Internet users.

4.2.6 Technology Transition and Transfer the Project

For dates of specific technology transition actions, please see all items listed in Section 4.2.2 marked [TTx].

In addition, we have done the following software releases:

[Soft1] Verfploter has been released at https://ant.isi.edu/software/verfploeter. [Soft2] Verfploeter/Plotter was released 2019-10-24 at https:/ant.isi.edu/software/verfploter/plotter to generate world-maps showing anycast catchment distributions.

[Soft3] Robert Story released Dnsroot-xtables on 2020-05-12. This code provides an iptables filter that drops non-TLD DNS queries in the kernel, reducing load on a root server that is under a DDoS attack with random DNS names. It was developed as part of the DDIDD project, but is relevant to PAADDoS.

[Soft4] Hang Guo released IoTSTEED-1.0 on 2020-05-19. IoTSTEED is a system that runs in edge (home) routers and observes IoT devices, learning their regular behavior and shutting them off if they are compromised and begin attacking. It was developed as work on another project, but is relevant to DDoS defense.

[Soft5] On 2020-07-01 and -02, John Heidemann released a new version of dnsanon_rssac (versions 1.13 and 1.14). Dnsanon_rssac computes RSSAC-002 statistics for B-Root; we use RSSAC-002 statistics to do early detection of DDoS events for curation. These releases addressed several small bugs in RSSAC-002v4 support: rcodes are now a toplevel element, and we made the time zone on dates explicit.

[Soft6] On 2020-07-01 Yuri Pradkin released dag_scrubber-0.4. This release changed the

default format to pcap (from ERF), added IP address translation as an option, and updated to the current version of cryptopANT.

4.2.7 Publications Over the Project

For context about these publications, please see items listed in Section 4.2.2 marked

[PubX]. Publications in prior reporting periods:

[Pub1] On 2019-06-13, ASM Rizvi and John Heidemann submitted "Dynamically Selecting Defenses to DDoS for DNS" for peer review.

[Pub2] On 2019-10-23, the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at ACM Internet Measurements Conference in Amsterdam, The Netherlands. This paper resulted in several presentations at related workshops.

[Pub3] On 2020-06-10, Wei, Marcel Flores, Harkeerat Bedi and John Heidemann published "Bidirectional Anycast/Unicast Probing (BAUP): Optimizing CDN Anycast" in the Proceedings of the IEEE Network Traffic Monitoring and Analysis Conference (Berlin, Germany, Jun. 2020).

[Pub4] On 2020-06-24, Hang Guo released the tech report " IoTSTEED: Bot-side Defense to IoT-based DDoS Attacks (Extended)" by Hang Guo and John Heidemann. Technical Report N. ISI-TR-738, USC/Information Sciences Institute, June, 2020. <https://www.isi.edu/%7ejohnh/PAPERS/Guo20b.html>. This paper was not directly supported by PAADDoS, but it is DDoS-related.

[Pub5] On 2020-06-24, ASM Rizvi released the arXiv report by ASM Rizvi, Joao Cern, Leandro Bertholdo, and John Heidemann. "Anycast Agility: Adaptive Routing to Manage DDoS". Technical Report N. arxiv:2006.14058v1, arXiv, June, 2020. <https://arxiv.org/2006.14058>.

[Pub6] On 2020-06-30, Giovane C. M. Moura, John Heidemann, Wes Hardaker, Jeroen Bulten, Joao Ceron and Christian Hesselman released "Old but Gold: Prospecting TCP to Engineer DNS Anycast (extended)" as Technical Report ISI-TR-740, USC/Information Sciences Institute

[Pub7] On 2020-07-27, the journal paper by Hang Guo and John Heidemann: "Detecting IoT Devices in the Internet" appeared online for *ACM/IEEE Transactions on Networking*, July, 2020.
<https://dx.doi.org/10.1109/TNET.2020.3009425>,
<https://www.isi.edu/%7ejohnh/PAPERS/Guo20c.html>.

4.2.8 Meetings and Presentations Over the Project

Meetings and presentations are to include meeting name, purpose, dates, location, attendees, and name of the presentation.

For context about these presentations listed here, please see items listed in Section 4.2.2 marked [PreX].

[Pre1] "Planning for Anycast as Anti-DDoS (PAADDoS)" is a talk prepared for the NCSC ONE conference in The Hague, Netherlands, 2019-10-02. We were uncertain if we would

have a slot to present and the DHS slots were allocated to existing projects, so we did not present this talk.

[Pre2] On 2018-07-15 John Heidemann presented "When the Dike Breaks: Dissecting DNS Defenses for DDoS" to the DNS Root Operators meeting in Montreal, Canada. (The talk was done remotely via teleconference.) This paper was joint work of Giovane Moura, John Heidemann, Ricardo Schmidt, Moritz Müller, and Marco Davids. The work on this paper is relevant to PAADDoS, but precedes the project start.

[Pre3] "Planning for Anycast as Anti-DDoS (PAADDoS)" , DHS Cybersecurity and Innovation Showcase, 2019-01-08. The showcase was postponed due to the U.S. Government shutdown, so this talk was not presented.

[Pre4] On 2019-03-19, John Heidemann presented "Planning for Anycast as Anti-DDoS (PAADDoS)" , DHS Cybersecurity and Innovation Showcase. This talk is a rescheduled version of [Pre3].

[Pre5] On 2019-03-26, ASM Rizvi presented "Dynamically Selecting Defenses to DDoS for DNS" at the ISI Graduate Student Symposium.

[Pre6] On 2019-10-15, Giovane Moura presented the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at RIPE-79 in Rotterdam, The Netherlands.

[Pre7] On 2019-10-23, Giovane Moura presented the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at ACM IMC 2019 in Amsterdam, The Netherlands.

[Pre8] On 2019-10-24, John Heidemann attended the DDoSD PI meeting in Utrech, Netherlands, where he presented "Planning for Anycast as Anti-DDoS (PAADDoS): Oct. 2019 Update".

[Pre9] On 2019-10-31, Wes Hardaker presented the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at DNS OARC 31, Fall 2019, in Austin, Texas, USA

[Pre10]On 2019-10-24, John Heidemann and Leandro Bertholdo met at ACM IMC to discuss Leandro's PhD research at U. Twente. His work will be part of the PAADDoS project there.

[Pre11]On 2019-11-26, Giovane Moura presented the paper "Cache Me If You Can; Effects of DNS Time-to-Live" , by Giovane Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker, at the Nordic Domain Days in Stockholm, Sweden.

[Pre12]On 2020-07-06, ASM Rizvi gave the talk "Anycast Agility: Adaptive Routing to Manage DDoS" as part of is PhD oral qualifying exam. This talk was based on joint work with John Heidemann, Joao Ceron, and Leandro Bertholdo and is work directly supported by PAADDoS.

[Pre13]On 2020-07-22, John Heidemann and Wes Hardaker hosted the DNS and Internet Naming Workshop, DINR 2020. This workshop was primarily focused on DNS analysis, but one source of DDoS attacks used in PAADDoS are DNS attack on B-Root.

[Pre14]On 2020-10-02, John Heidemann gave the talk "Anycast Latency: Goals and Measurements", at Amazon as an invited talk.

4.2.9 Issues or Concerns Over the Project

The COVID-19 virus caused USC to begin working from home as of March 18, 2020. We carried out project research using remote access to our servers and telecommunications tools for videoconferencing.

In October 2020 we requested a no-cost extension to extend the contract to 2020-12-31. This extension allowed us fully to support a graduate research student for the entire semester on one project.

5.0 CONCLUSIONS AND RECOMMENDATIONS

This section summarizes lessons learned at the conclusion of the project in December 2020.

5.1 Key Accomplishments and Next Steps

The PAADDoS project accomplished several significant project and program goals.

PAADDoS Developed New Tools to Map Anycast Catchments: building on our existing Verfploeter tool, we provided verfploeter_plotter to visualize the results (as described in Section 4.1.1).

PAADDoS Used These Tools to Map Anycast Catchments for DDoS Defense: by systematically varying routing and studying the resulting catchmentsk, the project mapped catchments and built a DDoS defense system. We summarized this system earlier (Section 4.1.2) and describe it in detail in [Rizvi20a].

PAADDOS Developed an Attack-Size Estimation Tool: To understand if a DDoS attack should be absorbed or spread to other sites one must know the attack size. The project developed an attack size estimation tool and evaluated it use against real attacks in testbed experiments. We summarized this tool earlier (Section 4.1.3) and describe it in detail in [Rizvi20a].

5.2 Key Results in Technology Transfer

The project had significant success in technology transfer, although more work is important.

We worked closely with B-Root and SIDN Labs. B-Root is using our anycast mapping tool today operationally to assist new anycast deployments (as described in Section 4.1.1), and SIDN has been using the tool to assess anycast catchments for the Netherlands country-code domain, .nl. In addition, extension to Verfploeter were developed by Cloudflare and are in operational use there, and we know of another major commercial anycast operator who is applying Verfploeter to their network.

We have released our tools as open source at the ANT project website https://ant.isi.edu/software/. We have also described the tools in public venues and documented them through peer-reviewed publications and technical reports.

This work was only possible with close collaboration with our colleagues at the University of Twente (Netherlands), SIDN, and B-Root. We thank them for their collaboration and recognize that joint effort as another form of technology transfer in both directions.

5.3 Conclusions

Overall, the PAADDOS project has advanced the state of the art in detection of Network/Internet Disruptive Events (NIDEs) and in measurement approaches to detect network outages in the data plane, routing plan, and services. We have provided data and results that have been directly used by at least three other groups. Our visualizations and data are being used operationally by the FCC today. At least three other groups have implemented outage detection systems inspired by our work. In addition, we have identified a number of future directions worthy of additional work. We are hopeful that DHS or some other funding source will recognize the benefits to see this work through to its next stages.

6.0 REFERENCES

[1] Hang Guo and John Heidemann. IoTSTEED: Bot-side Defense to IoT-based DDoS Attacks (Extended). Technical Report N. ISI-TR-738, USC/Information Sciences Institute, June, 2020. <https://www.isi.edu/%7ejohnh/PAPERS/Guo20b.html>.

[2] Hang Guo and John Heidemann. Detecting IoT Devices in the Internet. *ACM/IEEE Transactions on Networking*, V. 28 (N. 5), October, 2020. <https://dx.doi.org/10.1109/TNET.2020.3009425>, <https://www.isi.edu/%7ejohnh/PAPERS/Guo20c.html>.

[3] Giovane C. M. Moura, John Heidemann, Ricardo de O. Schmidt, and Wes Hardaker. Cache Me If You Can: Effects of DNS Time-to-Live. In *Proceedings of the ACM Internet Measurement Conference*, p. 101--115. Amsterdam, the Netherlands, ACM. October, 2019. <https://doi.org/10.1145/3355369.3355568>, <https://www.isi.edu/%7ejohnh/PAPERS/Moura19b.html>.

[4] Giovane C. M. Moura, John Heidemann, Wes Hardaker, Jeroen Bulten, Joao Ceron, and Christian Hesselman. Old but Gold: Prospecting TCP to Engineer DNS Anycast (extended). Technical Report N. ISI-TR-739b, USC/Information Sciences Institute, June, 2020. Released June 2020, updated April 2021. <https://www.isi.edu/%7ejohnh/PAPERS/Moura20a.html>.

[5] ASM Rizvi, Joao Ceron, Leandro Bertholdo, and John Heidemann. Anycast Agility: Adaptive Routing to Manage DDoS. Technical Report N. arxiv:2006.14058v1, arXiv, June, 2020. <https://arxiv.org/2006.14058>.

[6] Lan Wei, Marcel Flores, Harkeerat Bedi, and John Heidemann. Bidirectional Anycast/Unicast Probing (BAUP): Optimizing CDN Anycast. In *Proceedings of the IEEE Network Traffic Monitoring and Analysis Conference*, Berlin, Germany, IFIP. June, 2020. <https://www.isi.edu/%7ejohnh/PAPERS/Wei20a.html>.

LIST OF ABBREVIATIONS AND ACRONYMS

ACM Association for Computing Machinery

AMS Amsterdam (airport code)

ANSI American National Standards Institute

ANT Analysis of Network Traffic, a research group at USC/ISI, see

https://ant.isi.edu BGP Border Gateway Protocol

BOS Boston (an airport code)

CDN Content Delivery

Network

CNF The airport code for Belo Horizonte International Airport in Confins,

Brazil DC District of Columbia

DDIDD DDoS Defense In Depth for DNS, a research project at USC/ISI, see

https://ant.isi.edu/ddidd DDOSD DDoS Defense, a DHS HS&T Program

DETER A network testbed at USC/ISI, see

https://deterlab.org DHS Department of Homeland

Security

DINR DNS and Internet Naming Research Directions, a workshop held at USC/ISI, see https://ant.isi.edu/events/dinr2020

DNS Domain Name System

EARR Enabling Anycast in the Research Root, a DHS-supported project at USC/ISI, see https://ant.isi.edu/earr

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics

Engineers IMC Internet Measurement Conference

IP Internet Protocol

ISC Internet Systems Consortium

ISI Information Sciences Institute, part of

USC ITP Improvements to Prototype

LAX Los Angeles International (an airport code)

NCSC The National Cyber Security Centre of the Netherlands

NWO Nederlandse Organisatie voor Wetenschappelijk Onderzoek, the Dutch Research

Council OARC The DNS Operations Analysis and Research Center

OMB Office of Management and Budget

PAADDOS Plannning for Anycast as Anti-DDoS, this research project

PEERING An anycast testbed run out of Columbia University

PI Principal Investigator

RIPE Réseaux IP Européens, the European Regional Internet Registery

SIDN Stichting Internet Domeinnaamregistratie Nederland, the Netherlands Foundation for Internet Domain Names

TCP Transmission Control Protocol

TTA Technical Task Area

US United States

USA United States of America

USC University of Southern California