TANGLED: A Cooperative Anycast Testbed

Leandro M. Bertholdo*, João M. Ceron†, Wouter B. de Vries‡,
Ricardo de Oliveira Schmidt§, Lisandro Zambenedetti Granville¶, Roland van Rijswijk-Deij*, Aiko Pras*

* University of Twente, Enschede, The Netherlands
{l.m.bertholdo, r.m.vanrijswijk, a.pras}@utwente.nl

† SIDN Labs, Arnhem, The Netherlands
joao.ceron@sidn.nl

‡ Tesorion, Enschede, The Netherlands
wouter.devries@tesorion.nl

§ University of Passo Fundo, Passo Fundo, Brazil
rschmidt@upf.br

¶ Federal University of Rio Grande do Sul, Porto Alegre, Brazil
granville@inf.ufrgs.br

***Abstract*—Anycast routing has attracted interest in recent years as a technology for CDNs and anti-DDoS services. Most anycast studies conducted in the past relied on coarse measurement data, or are subjected to the collaboration of a global player affecting the experiment flexibility. In this paper, we present TANGLED, an anycast testbed where researchers can run experiments and better understand the impacts of their proposals on a global infrastructure. We also share our hands-on experience validating transit providers routing configurations. Our testbed offers a flexible and complete testing environment to evaluate the routing behavior of anycast networks in the wild. We provided tools that allow users to customize and reconfigure the anycast network, perform experiments, do active measurements, and collect data by using a platform specially designed for. The deployed infrastructure was designed to create industry and academy cooperation. TANGLED enables researchers to answer your research questions while allows transit providers to validate the implementation of complex routing agreements.**

***Index Terms*—Anycast Network, Network Measurement, Testing networks, Configuration Management, Routing Management.**

I. INTRODUCTION

IP anycast consists in announcing different copies of a service in the Internet using the same IP address, and trusting the Internet routing (*e.g.* BGP [1]) to forward and distribute traffic between service copies.

Initially proposed in 1993, IP anycast was originally used to help clients find the best application server in the Internet [2]. Since then, IP anycast has been widely employed for load balancing [3] [4] [5], in the DNS infrastructure [6] [7], and CDN cloud providers [8] [9] [10] [11], and, more recently, it has also been studied and deployed for DDoS mitigation [12] [13] [14] [15]. Today, anycast is used to support hundreds of services across the Internet [16] [17].

Although there is a large literature on IP anycast, carrying out real-world experiments with IP anycast is not an easy task. Typically, and understandably, operators do not allow for running tests on production networks and servers; and deploying a meaningfully large anycast network, consisting of various copies of a service widely and reasonably distributed across the Internet is beyond reach for most researchers. Building an IP anycast network is not a technically challenging task per se (in fact, there are many references and guidelines on how to do it [18] [19] [20]). However, the major roadblocks are the cost and time involved in the process of building a proper anycast network following the same practices of the industry, and retrieving trusted data from that network.

Based on experiences of our previous work in IP anycast, we argue that a testbed deployed in the wild is the most feasible and technically accurate way to run experiments. Testbeds are usually built on a collaborative way, where industry and academia together support research that benefit the Internet operations. Compared to other approaches and methodologies, such as using third-party datasets for research, testbeds commonly allow for changes in metrics, which enables the study of a given subject under different conditions.

In this paper, we introduce TANGLED[1], a world-wide, collaborative open-access IP anycast testbed. TANGLED ultimately aims to support research on anycast by academia and industry by making the deployment of anycast-related experiments viable to the overall community of network research and operation. Our testbed consists of various copies (*a.k.a.* anycast instances or anycast sites) distributed around the globe and co-located under different ASes, as well as a set of tools to: (*i*) provide a programmable anycast traffic engineering interface, able to control each individual anycast site visibility; (*ii*) map the distribution of traffic from clients to the anycast sites using million of vantage points; (*iii*) validate the BGP traffic engineering configuration on our transit providers; and (*iv*) measure and analyze result data from experiments. This paper present the infrastructure of TANGLED as of September

978-3-903176-32-4

[1] https://anycast-testbed.nl

2020. We are constantly looking for opportunities to expand our testbed by establishing new partnerships, as well as the deployment of new nodes.

The remainder of this paper is organized as follows. In section II we describe our testbed technical details on connectivity and infrastructure. In section III we show all preprogrammed testbed routing features available. In section IV we explain our data collection process and exported data format. In section V we state some experience we learned for running this testbed and how it helped our transit providers to identify configuration issues on its networks. In section VI we compare TANGLED with other research solutions available to anycast research.

II. THE TANGLED TESTBED

Configuring and deploying an anycast network is a process that involves a constant maintenance. Internet service providers (ISPs) and Internet exchanges (IXPs) change policies and infrastructure from time to time. However, TANGLED active measurement infrastructure allows to identify BGP routing configurations mistakes or relevant infrastructure changes made by ISP or IXPs where we have presence. This capability provide us a more trustable anycast testbed environment.

TANGLED consists of thirteen sites, most of these deployed through partnership with universities and academical networks, registrars, and transit providers. Some of our anycast sites are deployed within cloud commercial networks, with the goal to increase the coverage of our anycast network to regions where we currently have no partners. In the case of an anycast network for research purposes, we generally believe that the more sites the better, mainly if these sites are located within different ASes; more sites in different networks increase, for example, the possibilities of combinations for experiments and observation of routing dynamics. Therefore, we believe that cooperation is a key factor to keep the TANGLED testbed growing and with a meaningful number of relevant sites.

A. Historical Context

TANGLED was conceived in 2016, during a BGP hackathon organized by CAIDA/UCSD [21]. In that event, while developing their BGP project, the team "Anycast-1", with members from the University of Twente (UT) among others, discovered misconfigurations within the *Peering* [22] BGP testbed. That situation helped us understand the challenges on building an anycast network, and it was the main motivation for the UT researchers to start planning their own testbed infrastructure. The first release of the TANGLED was presented on RIPE73 [23].

In the following years, we expanded our community network around the testbed, deploying anycast sites around the world. Several researches were carried out along the years using the TANGLED network: anycast catchment studies [24] [25] and the tool called VERFPLOETER [26]; and several anti-DDoS studies from [13] [14] were carried out using our testbed. Moreover, the TANGLED testbed is actively being used in the projects SAND [27] and PaaDDoS [28] and some of our results direct applied to the industry [29] [30].

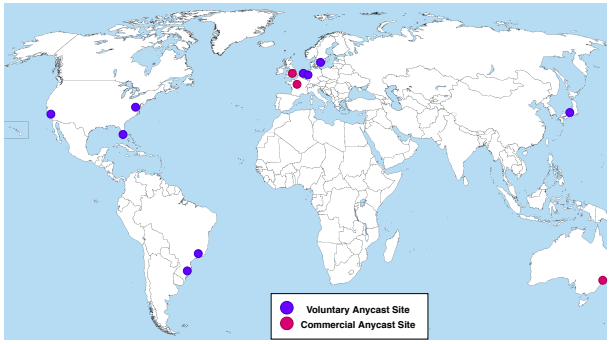

Fig. 1: Anycast sites provided by TANGLED.

B. Addressing Infrastructure

TANGLED owns AS 1149, and IPv4/IPv6 prefixes (145.100.118.0/23 and 2001:610:900::/40) provided by SURFnet–the Dutch NREN. Our both prefixes are RPKI signed and properly described on RIRs databases, increasing security of our routing environment and preventing the prefixes misuse. Multiple distinct experiments can be configured and executed at the same time in TANGLED by using smaller prefixes; for example announcing two /24 prefixes instead of our original /23 one, or even a fraction of the IPv6 address space.

C. Connectivity

Anycast networks have similar requirements to content distribution networks, aiming to connect directly to each AS on the Internet. So in our testbed we try to increase each site visibility connecting to more than on transit provider and IXPs. TANGLED has one master site used to consolidate data, and thirteen anycast sites deployed in Asia (1 site), Europe (6), South America (2), North America (3), and in Oceania (1), as depicted in Figure 1. Five sites are connected to IXPs, meaning that these sites have richer connectivity: both sites in Brazil (São Paulo and Porto Alegre) are directly connected to the Brazilian Internet Exchange Point (IX.br); the sites in Amsterdam, London and Paris have access to AMSIX, Linx and FranceIX, respectively. Table I details our transit providers and IXP connections. Some of our anycast sites share the same upstream provider, while others peer with various commercial and academic networks.

Since site connectivity have a direct relationship with the anycast catchment[2] [31], *i.e.* BGP might prefer to forward traffic to a more distant site but with better connectivity. This variety of connectivity provides valuable study cases for the testbed. Figure 2 shows the Huricane Eletric looking glass view of AS1149.

Since our goal is to create tailored experiments for anycast, we also have implemented tools for controlling and measuring systems. These tools are described in the next sections.

[2]Anycast catchment is defined by the distribution of source traffic as defined by BGP routing decisions, ultimately defining the set of sources an anycast site sees in its incoming traffic

Site ID	Location	Transit Provider	IXP	Peers
au-syd	Sidney Australia	Vultr (20473)	–	1
br-gru	São Paulo Brazil	Ampath(20080) ANSP(1251)	spo.IX.br	1892
br-poa	Porto Alegre Brazil	Leovin(262605) Nexfibra(264575)	poa.IX.br	218
dk-cop	Copenhagen Denmark	DK-Hostmaster (39839)	–	1
uk-lnd	London England	Vultr (20473)	Linx	1
fr-par	Paris France	Vultr (20473)	France-IX	1
jp-hnd	Tokyo Japan	Wide (2500)	–	1
nl-ams	Amsterdam Netherlands	Vultr (20473)	AMSIX	1
nl-arn	Arnhem Netherlands	SIDN (1140)	–	1
nl-ens	Enschede Netherlands	UTwente (1133)	–	1
us-los	Los Angeles United States	USC (4)	–	1
us-mia	Miami United States	Ampath (20080)	–	1
us-was	Washington United States	Los Nettos (226)	–	1

TABLE I: TANGLED sites location and connectivity.

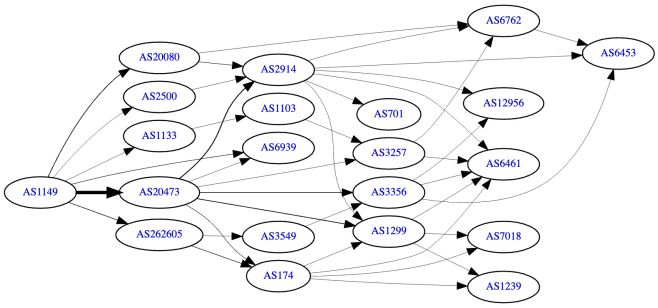

Fig. 2: Partial route propagation map (source:he.net).

III. TRAFFIC ENGINEERING ON TANGLED

IP anycast relies on BGP for the routing of users' traffic to the available anycast sites; in this context, the optimal situation is typically defined as users being routed to the topologically nearest anycast site. One of the challenges for anycast operators is not having complete control on catchment because of the complexity and limitations of BGP routing. However, BGP does have mechanisms to express routing preferences, ultimately influencing routing decision processes. For example, one can prioritize some paths over others. In TANGLED, we support two methods of BGP engineering: AS-path manipulation and community strings.

AS-path manipulation lies in making changes in the BGP path attribute. AS-path is used to implements loop avoidance in BGP. An AS-path carries a list of all ASes from the current site, back to the route originator, providing a rough distance estimation metric measured in number of AS hops. The AS-path manipulation can be done by: (1) *prepending*, decreasing the preference of a routing path by inflating its number of hops; (2) *poisoning*, indicating ASes to oppose a given path; or (3) *reverse prepending*, by inflating all but one paths.

	Prepend	No Peer	No Export	No Client	Selective Prepend	Selective Advertise
AS4	✓	–	–	–	–	–
AS226	✓	–	–	–	–	–
AS1133	✓	–	–	–	–	–
AS1140	✓	–	–	–	–	–
AS1251	✓	–	–	–	–	–
AS2500	✓	–	–	–	–	–
AS20080	✓	✓	✓	✓	✓	✓
AS20473	✓	✓	✓	–	✓	✓
AS39839	✓	–	–	–	–	–
AS262605	✓	✓	–	–	–	–
AS264575	✓	✓	✓	–	–	✓

TABLE II: Traffic Engineering options by transit provider

Community String is a label optionally informed with the prefix announcement, which is interpreted by the BGP neighbor and translated into an internal AS routing policy. Communities are widely supported by ISPs to delegate some of the BGP routing control to their customers. Although community labels are not standardized, some conventions do exist; for example, *well-known communities* map labels to routing policies such as *no-export* [32]. Communities can be propagated to all the neighbors of a BGP router, or can target a particular AS. *Selective communities* allow a specific routing policy to be applied only to one individual selected AS.

We classify the available community strings in TANGLED in the following routing policies:

- *Prepend*: send an inflated AS-Path to a neighbor.
- *noPeer*: do not send prefix to IXPs or private peering.
- *noExport*: do not propagate this announcement beyond the neighboring AS.
- *noClient*: do not send this prefix to ISP customers.
- *Selective Prepend*: ask to upstream/IXP to prepend our prefix when sending to a specific AS neighbor.
- *Selective Advertise*: send prefix only to a specific AS; or, send to all but a specific AS.

Table II shows that there is no homogeneity among TANGLED's transit providers in terms of BGP Engineering options. Such differences among ISPs is not considered an actual problem; it is rather a reflection of the freedom that ISPs have on defining how to support their respective clients.

A. Inter-domain Routing Programming

To simplify the routing management across the anycast sites, we developed an open-source tool named *tangled-cli*. Built on top of Bird [33] and ExaBGP [34], one can use *tangled-cli*'s interface to manage anycast site individually:

- perform regular BGP prefix site announcements
- withdraw the BGP prefix from any site
- performing AS-path prepending
- announce a specific community string to a neighbor
- get the configuration of all active anycast sites
- get the status of all BGP peers

Listing 1 shows examples of BGP routing configuration from the *tangled-cli*. The first command line configures a prefix announcement using the IPv6 prefix 2001:610:9000::/40

from the anycast site fr-par-anycast. In the second command line, we configure 20 path prepending on the IPv4 prefix 145.100.118.0/23 for the anycast site br-poa-anycast.

In addition to prepending and community, *tangled-cli* has other functionalities to help manage the anycast sites, such as list prefix, remove BGP policy, and withdraw BGP prefix.

```
$ tangled-cli -6 -A -t fr-par -r 2001:610:9000::/40
$ tangled-cli -4 -A -t br-poa -r 145.100.118.0/23 -P 20
```

Listing 1: tangled-cli interface

IV. Data Measurement and Analysis

There are multiple ways to measure anycast networks towards studies of performance and behavior [17] [35] [36] [37]. In the case of TANGLED, we deployed VERFPLOETER [37], which we describe next.

A. Anycast Mapping Measurements

VERFPLOETER actively probes IP addresses within a hit list (vantage points–VP) using ICMP ECHO requests, to map clients of a distributed service which is configured with IP anycast. Figure 3 shows the catchment mapping extracted from VERFPLOETER. ICMP ECHO requests are sent by one or more servers called *Pingers*; these servers may be, for example, actual anycast sites or other multi-purpose servers.

The source IP address used in the ICMP ECHO messages is the address configured in the anycast service. Active VPs replying to the ICMP request, set the destination IP address of their respective ICMP REPLY messages to that of the anycast service. Therefore, anycast sites will receive REPLY messages without actually sending an ECHO request. The set of received replies by each site defines their respective anycast catchment.

Measurement Duration.

The duration of an entire measurement depends on how large is the IP hit list, and also how frequent the ICMP ECHO requests are sent out to their destinations as well as how many *Pingers* are actively probing. One could easily probe the entire set of valid /24 networks within the Internet in minutes—our estimations is of 15 minutes for a measurement with just one *Pinger* and 6,5 millions IP addresses in the hit list. However, we strongly take care of measurements that send large amounts of ICMP requests within a short period of time because they can be understood as an abusive behavior. As described in [38], actively probing hosts in the Internet should not generate traffic that is discernible from the *traffic background noise*.

Vantage Points.

The accuracy of measurements in VERFPLOETER strongly depends on the number and distribution of VPs, and also on how responsive they are. Examples of hit lists that can be used in VERFPLOETER are those built in [38], or an Alexa's top-sites listing. In addition, geolocation of VPs can be based on any geoIP database/source of choice.

Catchment and Traffic Load.

Since each VP in a hit list can be mapped to a /24 network, we can estimate the traffic load each anycast site would receive in an actual operation. The accuracy of such an estimation, however, depends on how comprehensive the VPs hit list is. Moreover, if unknown, the distribution of traffic origins in such estimation would have to be uniform across all /24 networks.

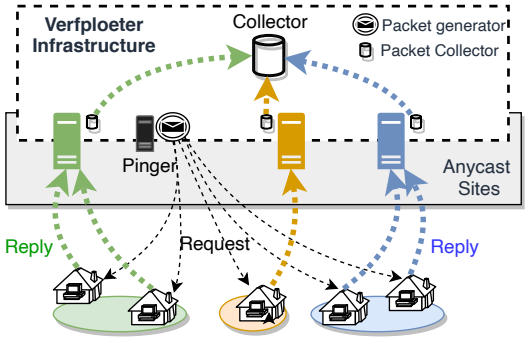

Fig. 3: VERFPLOETER and its vantage points.

Latency Measurements.

To enable latency measurements, VERFPLOETER inserts a timestamp on each outgoing ICMP ECHO request. When the ICMP REPLY is received at one of the anycast sites, the difference between the first timestamp and the receiving time is recorded. This time difference is a triangular round-trip time, similar to that of RTT concept.

B. Data Analysis

To explore the data generated from the measurements, we have developed tools to support that analyze. In particular, we are interested on analyzing the data produced by VERFPLOETER aiming to find the traffic distribution and catchment. A commonly used method to analyze volume of data is by using Jupyter notebooks. To make things simpler, we made available examples on Github [3] [4] and allow VP data be exported in comma separated value (CSV) format to be easily interchanged. Each round of measurement probes more than 6 millions networks and generates around 400MB uncompressed text data. Table III shows a summarized view of the measurement output.

Site	Time Diff	Target IP	Anycast IP	TTL	CC	ASN
au-syd	97.191805	1.1.1.2	145.100.118.1	52	AU	13335
au-syd	102.285587	1.0.0.230	145.100.118.1	52	AU	13335
au-syd	110.469751	1.0.7.1	145.100.118.1	52	AU	56203
au-syd	116.260893	1.0.4.4	145.100.118.1	52	AU	56203

TABLE III: Catchment data provided by VERFPLOETER.

To help deal with such amount of data, we provide a tool to quickly parse data provided by VERFPLOETER output and present the catchment distribution. Listing 2 show an example. The listing shows an anycast service using 6 sites and the respective number of replies that each site handled during the measurement. The site *us-los-anycast-01* has received 1,342,542 replies, which represent 37% of queries performed in the measurement. This means, that 37% of clients reach the mentioned site.

[3] https://github.com/joaoceron/verfploeter-ttl-investigation
[4] https://github.com/LMBertholdo/BQ-rtt

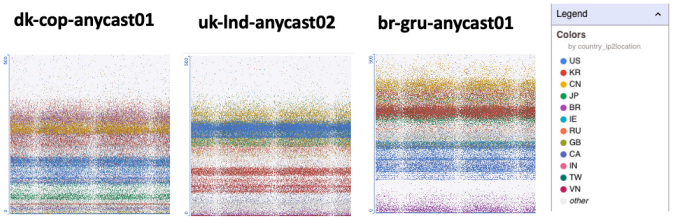

Fig. 4: RTT by site and country using Google BigQuery.

```
# sites| replies -  percentual
us-los | 1342542 -  37%  ████████████████████████
uk-lnd | 1123535 -  31%  ████████████████████
us-mia |  541846 -  15%  ████████
fr-par |  473867 -  13%  ██████
au-syd |   85475 -   2%  ■
jp-hnd |     321 -   0%  |
```

Listing 2: Quick TANGLED data analysis overview

Regular measurements can easily lead to big data problems, demanding to analyze a huge amount of data. To support this kind of investigation, we have written some codes able to upload measurement and use big data solutions, such as the *Google Big Query* platform. One example of this is the round-trip-time analysis, shown on Figure 4. This figure show individual round-trip time of million different vantage points, which site each one are choosing, and in which country this vantage point is located.

V. LESSONS LEARNED

While running an anycast testbed as a service, we identified some challenges and learned some lessons.

First, the Internet is dynamic and things break and get fixed without notification. After a year of operation, we were able to detect some operator's mistakes and evaluated how it affected our prefix visibility. We could sense our provider's equipment replacement by noticing performance degradation on individual anycast sites. Our health check procedure alerted such problems, and after phone contact all issues have been fixed. In anycast networks, detecting such problems is not so easy as appear, mainly because mostly available routing paths are just backup paths. Our first lesson learned: anycast sites need to run an individual, and automated baseline checkup procedure from time to time. To carry this out, we need an extra IP address space.

Our second lesson is about inter-domain routing and its slow convergence. When we use software defined networks (SDN) to define any inter-domain routing, we need to pay attention that BGP convergence is significantly faster than global forwarding table convergence. The forwarding plane convergence on all Internet routers is slow; around 10 minutes, and BGP "routing update" messages take more time than a "withdraw" message or an route announcement made for the first time.

Third, wide collaboration on Internet, as we are trying with TANGLED have some drawbacks. Since most of our anycast sites are deployed and maintained by partners, normally in a best-effort fashion, bring us limitations related to the operation of the infrastructure itself. This affect us when running long-term measurements. In general we register issues related to:

- limited peering control: we are submitted to our collaborator policies. Sometimes more flexibility is desired.
- detect packet loss means long period of problems: when we started to detect a packet loss in a path, to solve it we usually spend a month.
- unpredictable (temporary) unavailability of anycast sites: our ISPs have their own maintenance issues. So, if we need high availability on one site, we need to choose a "transit independent datacenter" to place this site. Some datacenters just allow a unique transit provider.

The limitation we registered mostly affected long term measurements. However, we have learned that carefully planning measurements circumvent problems such as temporary unavailability of anycast sites.

Forth lesson, the operational use of BGP communities is quite unstable. Configuration changes performed by upstream may affect the BGP communities effectiveness. In our experiments we noticed several cases of mistakes on BGP communities implementation. In one case some BGP communities just stopped working. In other case we identified we were not properly announced to one upstream of our upstream. In another, our prefix was mistakenly announced to one private peering and our packets were filtered by that peer.

Our Forth lesson lead us to your last lesson – collaboration means helping each other. So, we started using the testbed as a tool to help our partners. We identify the tooling we deployed at TANGLED works well as a third-party routing policy validation. We tested it on cases as new peering agreement, upstream change, or implementation of others business rules.

In Figure 5 we show a case where our transit used TANGLED to validate a new class of business to offer. In this policy they should permit access just to its clients, some selected peers and CDNs who permit to sell traffic to. We could together identify mistakes. Besides we are receiving routes correctly, some of our prefixes are leaking to other peers and we are getting access to all CDNs instead of just that allow sell traffic by a third party.

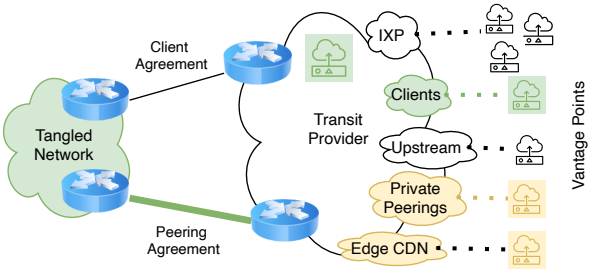

Fig. 5: Using TANGLED on routing agreement validation

We identify this situation by measuring the traffic asymmetry. This case helped us to get a strong bond with this partner and proof that cooperative anycast testbed can be pretty useful on routing policy validation.

VI. Related Work

Anycast research can be carried out by using simulators [3] [6], testbeds [7] [26] [15] or anycast networks in production [31] [29]. Anycast simulations are used in specific cases when you need to study site load and swarm and mobile catchment behaviors, usually in mobile and wireless networks. Anycast testbeds are normally used to Internet-related CDNs, DNS, and DDoS studies [26] [15].

Three distinct testbeds have been used for anycast tests so far. The first one is *Planetlab* [39], a testbed for overlay networks used to develop [40] a global anycast solution. Other is *Peering* [22], a BGP testbed widely used in Internet's BGP routing system research and for some anycast research [21] [15]. The last one is TANGLED, a testbed specific for anycast research and test. Over it several anycast studies are carried out by [23] [13] [14] [29] [27] [28] [15].

Even though it is possible to built one's own testbed even by renting capacity from some anycast or cloud provider; the whole anycast measurement setup for data collection still has to be built. In general the process of setting up, testing, and validating the whole testbed environment spend months. Instead of wasting time building one's own testbed, now researches can easily run their own anycast experiments and focus on improving their ideas and results. In similar ways, industry can benefit from this partnership too.

Acknowledgement

This project have the support of SIDNLabs and NSNetLabs and is founded by DHS HSARPA Cyber Security Division (HSHQDC-17-R-B0004-TTA.02-0006-I), Netherlands Organization for scientific research NWO (628.001.029), and CONCORDIA, the Cybersecurity Competence Network supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

References

[1] Y. Rekhter, T. Li, and S. Hares, "A border gateway protocol 4 (bgp-4)," Internet Requests for Comments, Tech. Rep. 4271, 2006.

[2] C. Partridge, T. Mendez, and W. Milliken, "Host anycasting service," Internet Requests for Comments, Tech. Rep. 1546, 1993.

[3] D. Katabi and J. Wroclawski, "A framework for scalable global ip-anycast (gia)," *SIGCOMM Comput. Commun. Rev.*, Aug. 2000.

[4] H. Ballani and P. Francis, "Towards a global ip anycast service," in *Computer Communication Review*, vol. 35, 2005, Conference Proceedings.

[5] M. J. Freedman, K. Lakshminarayanan, and D. Mazires, "Oasis: Anycast for any service," in *NSDI*, vol. 6, 2006, Conference Proceedings.

[6] G. Agarwal, R. Shah, and J. Walrand, "Content distribution architecture using network layer anycast," in *Proceedings. The Second IEEE Workshop on Internet Applications. WIAPP 2001.* IEEE, 2001.

[7] S. Sarat, V. Pappas, and A. Terzis, "On the use of anycast in dns," in *Proceedings of 15th International Conference on Computer Communications and Networks*. IEEE, 2006, pp. 71–78.

[8] E. Swildens, Sven-Johan, Z. Liu, and R. D. Day, "Global traffic management system using ip anycast routing and dynamic load-balancing," 2009, uS Patent 7,574.499B1.

[9] O. Spatscheck and et. al., "Multi-autonomous system anycast content delivery network," 2013, uS Patent 8,607,014B2.

[10] D. Shapira, E. Cohen, T. Bronshtein, E. Lehsem, and A. Ludmer, "Infrastructure distributed denial of service (ddos) protection," 2017, uS Patent US2017/03657A1.

[11] J. T. Maslak, "Anycast routing techniques in a network," 2020, uS Patent 0036781A1.

[12] G. C. Moura, R. d. O. Schmidt, J. Heidemann, W. B. de Vries, M. Muller, L. Wei, and C. Hesselman, "Anycast vs. ddos: Evaluating the november 2015 root dns event," in *Proceedings of the 2016 Internet Measurement Conference*, 2016, pp. 255–270.

[13] W. de Vries and et. al., "Anycast and its potential for ddos mitigation," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 2016, pp. 147–151.

[14] J. H. Kuipers, "Anycast for ddos," https://essay.utwente.nl/73795/1/Kuipers_MA_EWI.pdf, 2017, [Online; accessed 5-May-2020].

[15] A. Rizvi, J. Ceron, L. Bertholdo, and J. Heidemann, "Anycast agility: Adaptive routing to manage ddos," *preprint arXiv:2006.14058*, 2020.

[16] D. Cicalese, J. Auge, D. Joumblatt, T. Friedman, and D. Rossi, "Characterizing ipv4 anycast adoption and deployment," p. Article 16, 2015.

[17] D. Cicalese and D. Rossi, "A longitudinal study of ip anycast," *ACM SIGCOMM Computer Communication Review*, 2018.

[18] J. Abey and K. Lindqvist, "Operation of anycast services," Internet Requests for Comments, RFC Editor, Tech. Rep. 4786, 2006.

[19] N. Morris, "Anycast on a shoe string," https://ripe69.ripe.net/archives/video/180/, 11 2014, (Accessed 13-jun-2020).

[20] S. Jafferali, "Build your own anycast network in nine steps," https://labs.ripe.net/Members/samir_jafferali/build-your-own-anycast-network-in-nine-steps, (Accessed on 12-Jun-2020).

[21] A. Dainotti, E. Katz-Bassett, and X. Dimitropolous, "The bgp hackathon 2016 report," *SIGCOMM Comput. Commun. Rev.*, Jul. 2018.

[22] B. Schlinker and et. al., "Peering: An as for us," in *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*, 2014.

[23] R. NCC, "The impact of routing on anycast," https://ripe73.ripe.net/archives/video/1429/, 10 2016, (Accessed on 12-jun-2020).

[24] W. B. de Vries, "Improving anycast with measurements," https://ris.utwente.nl/ws/portalfiles/portal/159315216/thesis.pdf, 2019, [Online; accessed 12-Jun-2019].

[25] R. Sommese, L. Bertholdo, G. Akiwate, M. Jonker, R. van Rijswijk-Deij, A. Dainotti, K. Claffy, and A. Sperotto, "Manycast2: Using anycast to measure anycast," ser. IMC '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 456463. [Online]. Available: https://doi.org/10.1145/3419394.3423646

[26] W. B. De Vries and et. al., "Broad and load-aware anycast mapping with verfploeter," in *Internet Measurement Conference*, 2017.

[27] J. Ceron, "Sand project," https://www.sand-project.nl/, (On 18-oct-20).

[28] L. Bertholdo, "Paaddos project," http://paaddos.nl/, (Online 18-oct-20).

[29] W. de Vries and et. al., "Global-scale anycast network management with verfploeter," in *IEEE/IFIP NOMS*. IEEE, 2020.

[30] L. M. Bertholdo, J. M. Ceron, L. Z. Granville, G. C. M. Moura, C. Hesselman, and R. van Rijswijk-Deij, "Bgp anycast tuner: Intuitive route management for anycast services," in *2020 16th International Conference on Network and Service Management (CNSM)*, 2020.

[31] S. McQuistin, S. P. Uppu, and M. Flores, "Taming anycast in the wild internet," in *Proceedings of the Internet Measurement Conference*, 2019.

[32] J. Borkenhagen and et. al., "Policy Behavior for Well-Known BGP Communities," Internet Requests for Comments, Tech. Rep. 8642, 2019.

[33] O. Filip, L. Forst, P. Machek, M. Mares, and O. Zajicek, "Bird internet routing daemon," *NANOG-48, Austin, TX*, 2010.

[34] T. Mangin, "Exabgp - a new tool to interact with bgp," https://labs.ripe.net/Members/thomas_mangin/content-exabgp-new-tool-interact-bgp, 2010, [Online; accessed 13-May-2020].

[35] H. Ballani, P. Francis, and S. Ratnasamy, "A measurement-based deployment proposal for ip anycast," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, 2006, pp. 231–244.

[36] C. Huang, A. Wang, J. Li, and K. W. Ross, "Measuring and evaluating large-scale cdns," in *ACM IMC*, vol. 8, 2008, pp. 15–29.

[37] R. de Oliveira Schmidt, J. Heidemann, and J. H. Kuipers, "Anycast latency: How many sites are enough?" in *International Conference on Passive and Active Network Measurement*. Springer, 2017.

[38] X. Fan and J. Heidemann, "Selecting representative ip addresses for internet topology studies," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM, 2010, pp. 411–423.

[39] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman, "Planetlab: an overlay testbed for broad-coverage services," *ACM SIGCOMM Computer Communication Review*, 2003.

[40] M. J. Freedman, K. Lakshminarayanan, and D. Mazières, "Oasis: Anycast for any service." in *NSDI*, vol. 6, 2006, pp. 10–10.