Anycast and Its Potential for DDoS Mitigation

Wouter Vries, Ricardo Schmidt, Aiko Pras

Anycast and its potential for DDoS mitigation

Wouter B. de Vries, Ricardo de O. Schmidt and Aiko Pras

University of Twente, The Netherlands
{w.b.devries,r.schmidt,a.pras}@utwente.nl

Abstract. IP anycast is widely being used to distribute essential Internet services, such as DNS, across the globe. One of the main reasons for doing so is to increase the redundancy of the service and reduce the impacts of the growing threat of DDoS attacks. IP anycast can be further used to mitigate DDoS attacks by confining the attack traffic to certain areas. This might cause the targeted service to become unavailable only to a fraction of its users. In this PhD research we aim at investigating how IP anycast can be optimized both statically and dynamically to support the mitigation of DDoS attacks.

1 Introduction

IP anycast is an addressing and routing strategy in which multiple physical servers in the Internet are configured with the same logical IP address. This strategy has been widely used to achieve high-availability and redundancy of services over the Internet, such as DNS and CDNs. IP anycast takes advantage of the robustness of BGP (Border Gateway Protocol) routing that defines the catchment of each anycast instance. BGP helps to define the catchment of each anycast instance by, for example, mapping users to the topologically nearest anycast instance. However, anycast catchment has proven to be more chaotic mainly due to routing policies that are defined within and between Autonomous Systems (ASes) [2,9].

There may be multiple motivations for deploying an anycast service. Nowadays, however, redundancy and resilience of Internet services against cyber attacks has gained importance. Particularly resilience against Distributed Denial-of-Service (DDoS) attacks since their occurence and intensity have significantly increased in the recent years [1], and essential Internet services are among their common targets [5]. This problem is exacerbated by the fact that today anyone can perform DDoS attacks [6].

When a service such as DNS is anycasted, there is no single point of failure. An anycasted service has the advantage that when being subject to a DDoS attack, the service might become unavailable to a fraction of the Internet only. That is, the service might be unreachable to the specific "catchment areas" of the affected anycast instances.

Although there are clear benefits to using IP anycast, and it generally works well [3], it alone does not solve the DDoS problem altogether. For example, on November 2015 [5] the DNS root servers received so many requests (caused by a

DDoS) that it saturated the network connections to some of them. The impact of this particular attack was limited though, due to the sheer scale of the DNS root servers; 11 out of 13 root nameservers are anycasted. However, for other (non-)anycasted services the impact can be more severe. Examples of severe service degradation were recently reported by RIPE through their DNS-WG mailing-list[1]: unusual amount of incoming traffic on the authoritative servers for RIPE DNS services on 14-Dec-2015 and on 14-Jan-2016. Recently, also the ccTLD DNS infrastructure of Turkey was attacked, causing severe service degradation [8]

In this PhD research, we will investigate how IP anycast deployments can be optimally planned and used to support service resilience against DDoS attacks. In the following we describe our main research goal, research questions, and planned approaches (§ 2). We also describe our first steps on building a global IP anycast service for our research (§ 3).

2 Goal, Research Questions, and Approach

The goal of this PhD research is *to investigate methods to optimize anycast deployments in order to improve service resilience against DDoS attacks.* To meet our goal we define four research questions.

First, to gain a more complete understanding of how operators currently mitigate DDoS attacks we define **(RQ1)** as *what are the current DDoS mitigation strategies in use by operators of critical Internet infrastructure.* Our approach will be focused on talking with operators, mainly those involved in the research, to understand their procedures and to be able to tailor improvements to them. To gain insight into the routing changes that will affect the catchment of anycast network when instances are added or removed, we define our second research question as **(RQ2)**: *what impact does the deployment of an anycast node in a given anycast network have on the overall catchment?*. To answer this question we will perform active and passive measurements on a real anycast deployment. We are deploying our own experimental anycast testbed, comparable to PEERING[7]. This testbed will allow us to announce and withdraw IP prefixes (both IPv4 and IPv6) from each anycast location. We will use the RIPE Atlas [4] framework to perform the active measurements This framework will allow us to closely monitor the effects of anycast node deployment from the perspective of thousands of vantage points worldwide. In addition, we will analyze the deployment from the BGP perspective using passive measurement data, provided by services such as BGPmon, and RIPE's Routing Information Service (RIS).

The knowledge obtained from RQ1 and RQ2 will be used to support anycast planning and instances placement targeting resilience against DDoS attacks. This leads us to our third question **(RQ3)**: *in what ways can the catchment of an anycast network be influenced to increase resilience against DDoS attacks?*. By analyzing the data obtained from RQ2 we attempt to find ways of optimizing

[1] https://www.ripe.net/mailman/listinfo/dns-wg/

the placement of nodes, aiming at increasing resilient against DDoS attacks. The key challenge is the fact that BGP routing is influenced by many, both technical and non-technical, factors. Potential methods will be verified in practice by implementing them using the anycast testbed and performing attacks on our own infrastructure. In addition, we will analyze the source of major DDoS attacks to determine if these are mostly located in certain areas. This will further assist in optimizing the anycast catchment for mitigation.

Finally, we determine if it is possible, and to what extent, the anycast catchment can be changed dynamically to further strengthen the DDoS mitigating property of an anycast network. For example by actively adding and/or removing instances during a DDoS attack near the source of attack traffic. Therefore, we define our fourth and final research question **(RQ4)** as: *how can service resilience be positively influenced by dynamically changing the composition of the anycast network?*. The results from RQ1, RQ2 and RQ3 as well as the operational experience gained using the anycast testbed will all contribute to answering RQ4. A potential solution is the deployment of inactive (ie, sleeping) instances that are activated on demand in the case of an attack. This setup can potentially lead to reduced operational costs as compared to the static approach of RQ3. The challenge lies in the fact that setting up anycast instances is not trivial because it might depend on routing policies and peering agreements involved in the anycast IP prefix announcement.

3 Preliminary Steps

As described above, one of the key components of this research plan is the anycast testbed. There is an existing testbed called PEERING [7], which provides the sort of functionality that is required for the research that we intend to carry out. However, access is limited in duration and in functionality, in the sense that experiments are very bandwidth limited. Therefore, we have started the development of a new anycast testbed in collaboration with SURFnet (the Dutch NREN). Having access to this testbed will allow us to perform experiments without having to rely on models that may or may not be an accurate representation of reality. During the past months we have obtained a /24 IPv4 prefix and a /48 IPv6 prefix, which are of a sufficient size to be announcable through BGP. Furthermore, we have started development of an anycast management webinterface (TANGLER) that will allow for easy control of the IP prefixes announcement from our anycast instances. The intention is that it will also allow advanced experiments to be performed by scheduling route announcements and withdrawals.

Figure 1 shows the locations of the (planned) anycast instaces of our testbed. Nodes are configured using an orchestration tool (Ansible), which makes it trivial to add new instances. Management occurs through a single management node to which each of the anycast instances maintains a VPN-connection. The BGP announcements for each of the anycast instances can currently be controlled through a webinterface running on the management node. In the future we will

also focus on creating a more local anycast network in Europe, constisting solely of European nodes. This will allow for studies on local impacts of DDoS mitigation and routing policies. Once our anycast testbed is fully operational, we plan to open the access (restricted by request and nature of research) to other researchers.

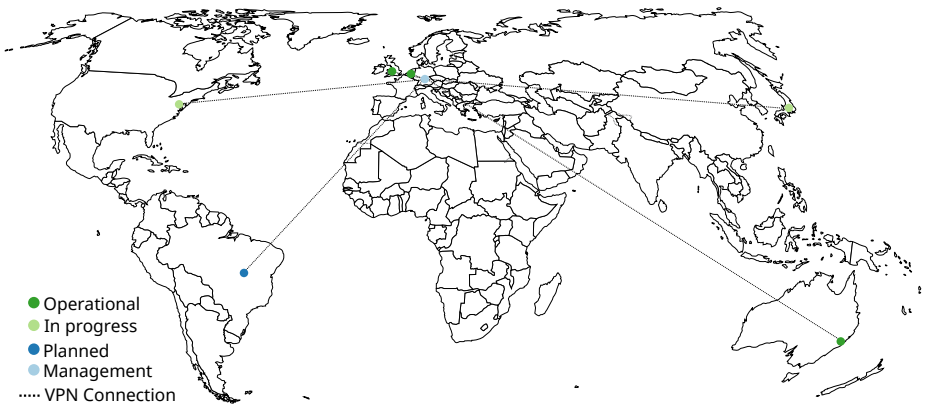

Fig. 1. Map of (planned) anycast nodes

4 Final Considerations

The PhD research outlined in this paper is planned to be carried out in a period of four years, which has started in late 2015 and will end in 2019. The preliminary steps (§ 3) have been carried out in the first six months.

Acknowledgements. This research is partially funded by SIDN and NLnet Labs through the projects DAS (http://www.das-project.nl) and SAND (http://www.sand-project.nl), by the EU FP7 FLAMINGO NoE (318488), and the SURFnet Research on Networks project.

References

1. Akamai: Q3 2015 state of the internet security report (2015), https://www.akamai.com/us/en/about/news/press/2015-press/akamai-releases-third-quarter-2015-state-of-the-internet-security-report.jsp
2. Anwar, R., Niaz, H., Choffnes, D., Cunha, I., Gill, P., Katz-Bassett, E.: Investigating interdomain routing policies in the wild. In: Proceedings of the 2015 ACM Conference on Internet Measurement Conference. pp. 71–77. IMC '15, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2815675.2815712

3. Liu, Z., Huffaker, B., Fomenkov, M., Brownlee, N., claffy, k.: Two days in the life of the dns anycast root servers. In: Uhlig, S., Papagiannaki, K., Bonaventure, O. (eds.) Passive and Active Network Measurement, Lecture Notes in Computer Science, vol. 4427, pp. 125–134. Springer Berlin Heidelberg (2007), http://dx.doi.org/10.1007/978-3-540-71617-4_13
4. NCC, R.: Ripe atlas (2016), https://ripe.atlas.net
5. Root Server Operators: Events of 2015-11-30 (2015), http://root-servers.org/news/events-of-20151130.txt
6. Santanna, J.J., Sperotto, A.: Characterizing and mitigating the ddos-as-a-service phenomenon. In: Monitoring and Securing Virtualized Networks and Services, pp. 74–78. Springer (2014)
7. Schlinker, B., Zarifis, K., Cunha, I., Feamster, N., Katz-Bassett, E.: Peering: An as for us. In: Proceedings of the 13th ACM Workshop on Hot Topics in Networks. p. 18. ACM (2014)
8. Sozeri, E.K.: Turkish internet hit with massive ddos attack (2015), http://www.dailydot.com/politics/turkey-ddos-attack-tk-universities/
9. Teixeira, R., Shaikh, A., Griffin, T., Rexford, J.: Dynamics of hot-potato routing in ip networks. SIGMETRICS Perform. Eval. Rev. 32(1), 307–319 (Jun 2004), http://doi.acm.org/10.1145/1012888.1005723