1 Problem

This paper explains the development of a new technique to measure the **expansion of Hypergiants(HG)' off-nets**. Key observations, Future Enhancements, limitations and other key points about this methodology are discussed in paper. From previous studies, results are **limited to specialised HG** - cannot be generalised. This problem gave rise to a generic and easy way to measure HG's off-nets using **TLS certificate**. Author mainly focussed on 4 HG's with off-nets (Google, Netflix, Facebook, Akamai), analyzed their footprint, scaling by region, type of networks and coverage.

2 Contributions

Author conducted various experiments - analyzing corpuses of scanned certificates to differentiate HG servioce hosted on third party platform. Author listed all the challenges, limitations and also performed manual work to identify and exclude the scanned certificates generated by proxy service. Author generated statistics, conducted survey among HG operators to verify the results obtained. Author came up with possible future approaches and enhancements for Hypergiant expansion. Author conducted experiments and unveiled the strategies behind expansion and reasons for shrink in deployment.

3 Conclusions & Support

Author while performing experiments used TLS certificates(X.509) to measure the off-net footprint. Each HG has a different deployment strategies(using own infrastructure, third-party CDN) which led to challenges. So, Author had to figure out a way to generalize, create a footprint for expansion of HG. Cloufare-issued certificate should be manually eliminated. In this techniques, valid certificates are used and invalid certifcates are eliminated using validity field in TLS certificate. Firstly, We must scan its on-nets and understand the **TLS fingerprints**(input the organization name, TLS scans all IP addresses bound to that name). Then, search for the TLS fingerprint in **scans of off-net** IP addresses to identify candidates - to search for the presence of certificate from HG on IP addresses outside HG. Next, understanding the **HG's HTTP headers** by scanning on-nets - perform manual classification and validation to find header fingerprints that identify the HG's web servers - excludes off-net candidates. Finally, **Confirm the candidate** by scanning the HTTP header fingerprints - classify off-nets if there is match in fingerprint. Use IP to AS mapping. Rapid7 for IPv4 scans on port 443, corpus of available HTTP headers are used for conducting experiments for validation. **ZGrab2 tool** was used to capture the HTTP header and TLS certificates. Author validated results by comparing to earlier results, surveying HG operators active measurement validation, comparing scanning corpuses. From Statistics, We can infer the following data : Cloudfare is misidentified as having off-nets. While studying longitudinal growth, Facebook has grown rapidly, Netflix growth was constant(manual investigation due to its complexity). APNIC dataset was used to investigate HG's off-net footprint growth in different regions. Facebook has an aggressive expansion over all regions considered for analysis While, Netflix and google has linear growth in Europe and Asia. To Conclude, Networks that hosted top-4 HG's are willing to host more in future. The number of ASes increased by **50%** in 7 years span.

4 Likes

Improved end-user performance(lower RTT). Opportunity to work on extended services(5G) to better deal with traffic. Discussion of possible approaches to hide the identity for security reasons.

5 Dislikes / Disagreements

The new methodology will not work of IPv6 address. Manual effort required to identify, remove proxy certificates (cloudfare). Reverse proxies, cache misses can confuse confirmation with headers.