Can we break the Internet?: A Robustness Analysis of the Internet Exchange Points (IXP) Network Graph.

Alexandra Ibarra
NIC Labs, Universidad de Chile, Chile
ale@niclabs.cl

Javier Bustos-Jiménez
NIC Labs, Universidad de Chile, Chile
jbustos@niclabs.cl

Abstract

Internet peering is the contract between two autonomous systems (AS) that agree to exchange traffic and traffic routes through a physical link, it is a multi-tier hierarchy where the first tier (of about 10-20 nodes) are connected with a clique of peering links, second tier are customers of the first, and residential and small business access are in the third tier. Therefore, it is natural to think that the peering exchange network (IXP) can be seen as the backbone of the Internet itself. Then, it is very important to study and analyze its robustness.

In this work we will study IXP network robustness under targeted attacks. Choosing the "right" node to disconnect under a greedy strategy, we will compare how much damage is produced by that node disconnection and we will compare how fast we can decouple the IXP network using the following strategies: selecting the node with the higher degree, with higher betweenness centrality, the higher degree in a 2-core network, and the node with higher collective influence.

Our work shows that the best algorithm for limited "strikes" in a targeted attack is selecting the node by higher betweenness. However, if a quick attack as important as precision, and having limited CPU resources, the best strategy is to select the nodes with higher degree.

1 Introduction

Internet peering is the contract between two autonomous systems (AS) that agree to exchange traffic and traffic routes through a physical link. The authors of [DD10] state that "*The core of the Internet is a multi-tier hierarchy of Transit Providers (TPs). About 10-20 tier-1 TPs, present in many geographical regions, are connected with a clique of peering links. Regional (tier-2) ISPs are customers of tier-1 TPs. Residential and small business access (tier-3) providers are typically customers of tier-2 TPs*". Therefore, it is natural to think that the peering network exchange network (IXP) can be seen as the backbone of the Internet itself.

Since their correct functioning requires that the network is properly connected, it is of great importance to study their ability to resist failures (either unintentional or targeted attacks). This ability is called robustness.

We consider that an "adversary" should plan a greedy strategy aiming to maximize the damage with minimum number of strikes. Thus, in this article we discuss the performance of attacks based on the node betweenness centrality metric [BMSBJ12] over the Internet Backbone (the network formed by Internet exchange points, IXP), also comparing the targeted attack performance against the optimal network decoupling algorithm MinSum [BDSZ16].

The article is organized as follows: next section presents related work, followed by the methodology for collecting data and creating the IXP network

(Section 3), and the analysis of IXP network as a graph (Section 4). Conclusions are presented in Section 5.

2 Related work

The idea to consider an IXP-based network as "the Internet backbone" is not new; It has previously been used as part of the "internet core" to study the inter-AS traffic patterns and an evolution of provider peering strategies [LIJM$^+$11], to optimize the content delivery from Google via direct paths [CSR$^+$15] and the Internet Backbone Market [BFBS05].

To study the robustness of a network, its evolution against failure must be analyzed. On real–world situations, networks may confront random failures as well as targeted attacks. For the latter, two main categories of attacking strategies have been defined: simultaneous and sequential attacks [HKYH02a]. Simultaneous attacks choose a set of nodes and remove them all at once while sequential attacks choose a node to remove and given the impact of this removal it chooses another node, proceeding iteratively.

On [Est06] it was found that targeted attack can be more effective when they are directed to bottlenecks rather than hubs. On [BRSBJ15] authors present partial values of R-index while nodes are disconnected, showing the importance of a well chosen robustness metric for performing the attacks.

For a better understanding of network attacks and strategies, see [HKYH02b, MR06, RW10, SSYS10].

3 Building the Internet backbone graph

From `peeringdb.com` we collected the autonomous systems (AS) from every Internet Exchange Point (IXP) and defined them as graph nodes, where there is an edge between any pair of nodes if and only if there is a physical connection (e.g.: fiber) between them. Figure 1 shows the resulting Graph, which has 786 nodes and $20,422$ edges.

4 Network Analysis

In our targeted attack, we start testing a sequential attack on our IXP network with two well known metrics: degree and betweenness centrality. At each strike, the next node to disconnect was the one with the highest metric value. Notice that in the former the nodes are sorted by degree at the first iteration and in the latter betweenness centrality are recalculated after each disconnection. It is widely accepted to use those metric, because it reflects the importance of an node in the network [IKSW13]. Also, attack strategies are compared by means of the *Unique Robustness Measure* (R-index) [SMA$^+$11], defined as:

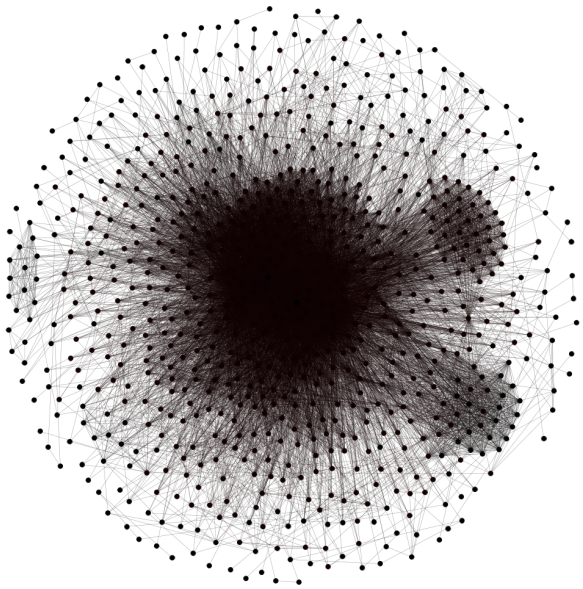

Figure 1: IXP Peering Graph

$$R = \frac{1}{N}\sum_{Q=1}^{N} s(Q), \tag{1}$$

where N is the number of nodes in the network and $s(Q)$ is the fraction of nodes in the largest connected component after disconnecting nodes using a given strategy. The higher the R-index, the better in terms of robustness.

In order to use more modern metrics, we compared the performance of both previous metrics against CoreHD [ZZZ16] and Collective Influence (CI) [MMB$^+$16] algorithms. CoreHD is based on the idea that, in a power-law network, there is a high number of nodes with degree 1 that will not contribute a network dismantling, thus first the 2-Core (nodes with degree ≥ 2) is built and then the node with higher degree is removed.

Collective Influence is based on the idea of finding the minimal set of maximal influencers in a network aiming to remove such set, more precisely: "*the most influential nodes in a complex*

network form the minimal set whose removal would dismantle the network in many disconnected and non-extensive components" [MMB$^+$16]. Following the recommendations of [BDSZ16] at each iteration the node with highest CI_2 value (calculating CI for each node using a radius of 2) is removed.

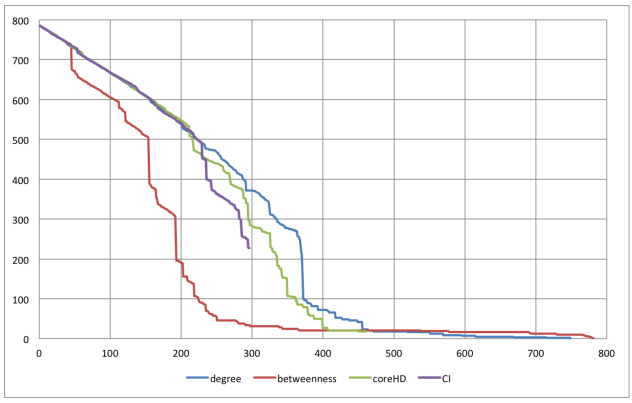

Figure 2: Largest component size. In the plot x-axis is the iteration, and R-index is the area below curves.

Plot in Figure 2 gave an idea for the best algorithm having limited "strikes" in the targeted attack, that is, selecting the node with higher betweenness. 20% of "Internet" is disconnected after removing 10% of the nodes and around half of the "Internet" is disconnected after removing just a 20% of the nodes. However, if a quick attack is important as precision, and having limited CPU resources (such as, only one desktop computer for strategy chosen), it seems that choosing the nodes with higher degree is the best strategy (Figure 3).

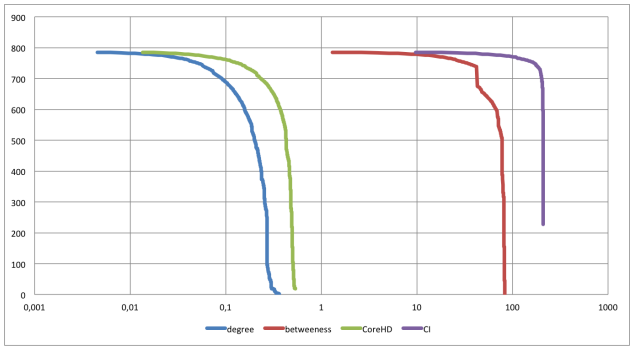

Figure 3: Largest component size. X-axis is in seconds since the beginning of the algorithm, and Y-axis is the larger connected component size.

5 Conclusions and Future Work

In this work we have presented how robust the Internet backbone (the peering AS network) would be if an adversary can choose wisely which AS node link will aisle (or if it is DDoS-ed, or if a very unlucky accident happens). Following the recommendations, the chosen one would be the node with a higher metric value such as degree, betweenness, or collective influence.

Our work has shown that the best algorithm for limited "strikes" in a targeted attack is selecting the node with higher betweenness. However, if a quick attack is important as precision, and having limited CPU resources, the best strategy is to select the nodes with the higher degree.

As future work we plan to apply similar studies to other Internet infrastructures, such as country-based fiber interconnection, submarine Internet cables, etc. Also, we plan to improve the metrics for robustness reflecting both the infrastructure and the user perception.

References

[BDSZ16] Alfredo Braunstein, Luca Dall'Asta, Guilhem Semerjian, and Lenka Zdeborová. Network dismantling. *Proceedings of the National Academy of Sciences*, 113(44):12368–12373, 2016.

[BFBS05] Paolo Buccirossi, Laura Ferrari Bravo, and Paolo Siciliani. Competition in the internet backbone market. *World Competition*, 28(2):233–252, 2005.

[BMSBJ12] Nicolás Ignacio Bersano-Méndez, Satu Elisa Schaeffer, and Javier Bustos-Jiménez. Metrics and models for social networks. In *Computational Social Networks*, pages 115–142. Springer, 2012.

[BRSBJ15] I. Bachmann, P. Reyes, A. Silva, and J. Bustos-Jimenez. Miuz: measuring the impact of disconnecting a node. In *2015 34th International Conference of the Chilean Computer Science Society (SCCC)*, pages 1–6, Nov 2015.

[CSR+15] Yi-Ching Chiu, Brandon Schlinker, Abhishek Balaji Radhakrishnan, Ethan Katz-Bassett, and Ramesh Govindan. Are we one hop away from a better internet? In *Proceedings of Internet Measurement Conference*, pages 523–529. ACM, 2015.

[DD10] Amogh Dhamdhere and Constantine Dovrolis. The internet is flat: Modeling the transition from a transit hierarchy to a peering mesh. In *Proceedings of Co-NEXT*, pages 21:1–21:12, New York, NY, USA, 2010. ACM.

[Est06] Ernesto Estrada. Network robustness to targeted attacks. the interplay of expansibility and degree distribution. *The European Physical Journal B-Condensed Matter and Complex Systems*, 52(4):563–574, 2006.

[HKYH02a] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.

[HKYH02b] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.

[IKSW13] Swami Iyer, Timothy Killingback, Bala Sundaram, and Zhen Wang. Attack robustness and centrality of complex networks. *PloS one*, 8(4):e59613, 2013.

[LIJM+11] Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian. Internet inter-domain traffic. *ACM SIGCOMM Computer Communication Review*, 41(4):75–86, 2011.

[MMB+16] Flaviano Morone, Byungjoon Min, Lin Bo, Romain Mari, and Hernán A Makse. Collective influence algorithm to find influencers via optimal percolation in massively large social media. *Scientific reports*, 6, 2016.

[MR06] Wojciech Molisz and Jacek Rak. End-to-end service survivability under attacks on networks. *Journal of Telecommunications and Information Technology*, pages 19–26, 2006.

[RW10] Jacek Rak and Krzysztof Walkowiak. Survivability of anycast and unicast flows under attacks on networks. In *International Congress on Ultra Modern Telecommunications and Control Systems*, pages 497–503. IEEE, 2010.

[SMA+11] Christian M Schneider, André A Moreira, José S Andrade, Shlomo Havlin, and Hans J Herrmann. Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences*, 108(10):3838–3841, 2011.

[SSYS10] Ali Sydney, Caterina Scoglio, Mina Youssef, and Phillip Schumm. Characterising the robustness of complex networks. *International Journal of Internet Technology and Secured Transactions*, 2(3-4):291–320, 2010.

[ZZZ16] Lenka Zdeborová, Pan Zhang, and Hai-Jun Zhou. Fast and simple decycling and dismantling of networks. *Scientific reports*, 6, 2016.