A Glance at Physical Connectivity and Internet Resilience

Shaddi Hasan Justine Sherry Kristin Stephens
University of California, Berkeley*

Draft: Please Do Not Distribute

ABSTRACT

Internet connectivity is an integral component of modern commerce and communication. Loss of Internet connectivity can shut down industries, limit the spread of information, and undermine free speech. However, physical bottlenecks in the Internet's structure leave it in many cases vulnerable to disconnection. In this paper, we investigate where these physical bottlenecks lie, leaving network communucation suceptible to interruption in cases of disaster or direct attack. Our analysis estimates that...

1. INTRODUCTION

The United States government defines *critical infrastructure* as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters." [1] Internet connectivity, a fundamental requirement for modern communication, is undoubtedly such a system. Businesses rely on such connectivity for communication with customers, coordination within their enterprise, and electronic commerce. Governments rely on the Internet for [**blah blah blah, hence Internet resilience is important**].

In this paper, we provide a brief glance at Internet resilience by focusing on a model of Internet Exchange Points, geographic locations where multiple networks converge to interconnect. An attack on one of these exchange points could lead to disconnectivity between the networks who exchange traffic at that location. Building on prior work which develops techniques for identifying formal Internet Exchange Points (IXPs) [4], discovering Points of Presence (PoPs) [9], and pinpointing border routers [**?**], we develop an AS connectivity graph that focuses on the locations where peering takes place. We then consider the behavior of an adversary who seeks to maximize damage to this connectivity graph. Such an adversary might wish to disconnect two Tier 1 networks, isolate a large number of networks, or partition a geographic region from the rest of the Internet. We consider each in turn.

Our results estimate that ...

We are not the first to evaluate Internet resilience to failures [12, **?**]. To the best of our knowledge, our contibutions are twofold.

First, we consider physical connectivity points, rather than logical links between networks. Previous work focused on the impact of severing logical links, that is, declaring that two networks had been entirely disconnected. This overestimates realistic damage in some cases, and underestimates in others. For example, it is highly unlikely that two Tier 1 networks would be partitioned in any single event. These networks have global footprints and connect at multiple physical locations. Thus, disconnecting Tier 1 networks is an overestimate of damage in all scenarios except a coordinated attack. On the other hand, disconnecting single logical links ignores the physical reality that any disaster that strikes a link in shared infrastructure such as an IXP is likely to impact a large number of links. In this case, modeling failure of a single logical link is an underestimate. We argue that focusing on physical connectivity points is a more realistic model of the impact of disaster.

Second, we consider resilience in an adversarial setting. Recent events in Egypt [**?**] and other countries involved government intervention to sever Internet access in order to limit communication between revolutionaries and the outside world. Further, the criticality of Internet communication makes it a prime target for terrorist attack. Attacks by any human entity may involve damage to one or more physical locations. Hence, our analysis is a superset of previous work which focused primarily on natural disaster or sideffects from events in a single location.

Before we move forward, we clarify the scope of our goals. Valuable evaluations of AS-level connectivity graphs show that traceroute-based topologies like those that we rely upon are in many ways incomplete [10]. For instance, policy compliant routing ensures that measurements made with only limited vantage points cannot observe peering relationships between networks where neither network contains a measurement vantage point. Further, 'backup links', which are provisioned for the case of failure but otherwise unused, cannot be observed since no traffic flows across these links when the primary links are available. These and other impedi-

*Authors listed alphabetically.

ments mean that any analysis over measurement-based graphs may be missing critical information. Thus, the results of our study should not be considered hard and fast projections of Internet connectivity. Instead, we aim only to provide *estimates* and *bounds* on the impact of attack on Internet infrastructure.

The remainder of the paper is organized as follows. Section **??** discusses our dataset and model of the physical connectivity of Internet infrastructure. Section **??** provides the algorithms we used in analyzing this model. Section **??** describes our discoveries from applying these algorithms. Finally, we discuss related work in § **??** and conclude in § **??**.

2. CONNECTIVITY MODEL

What our data is. How we piece it together.

Evaluation of Model

- survey random network providers and ask them if what we found was correct
- compare physical links discovered to logical connectivity graph (CAIDA provides this) - what fraction of logical links did we observe? For Tier-1's? For Tier-2's? For stub networks?

3. ALGORITHMIC ANALYSIS

How we do:

1. Easy peasy: partition Tier-1's
2. Maximize number of nodes that are completely isolated
3. Focus partition to a geographic region

4. RESULTS

Graphs and stuff.

Comparison to Recent Events

[**discuss Egypt and Iran?**]

5. RELATED WORK

Our work builds on and takes inspiration from research in Internet resilience analysis, experience from Internet outages, PoP-level Internet topology measurement studies, and network infrastructure security policy.

Resilience Analysis. Comprehensive analysis of Internet resilience remains beyond reach due to limited access to global routing and topology data. However, limited studies provide insight into the impact of logical link failures and opportunities to make the AS graph more robust to these failures.

Wu et. al [12] provide the most in-depth analysis of Internet resilience under *logical* link failure. Using an AS-level graph, they removed one or more peering relationships and evaluated the availability of policy-compliant paths between impacted networks before and after the logical link failure.

Omer et. al [11] consider undersea cables as capacity bottlenecks for Internet connectivity between continents. Like us, they look for constraints in the physical, rather than logical connectivity graph. However, their model focuses on inter-continental connectivity rather and does not focus on IXPs as correlated failure points.

[**justine: hey ksteph, can you add a line or two for each of these that provide a direct comparison to what we do and why it's different?**] Albert et al. [3] studied two different complex networks: Erdos-Renyi (ER) and scale-free. An ER model produces a network with an exponential tail and a scale-free has a power-law tail for node degree. Against random node removal the scale-free model had a high degree of tolerance, while the ER model was not. However for a deliberate attack of removing the most connected nodes the scale-free model quickly deteriorates and the ER model is effected the same as if they were randomly removed.

Dolev et al. [5] looked at an AS-level graph based on BGP policy directionality and connectivity. They found that the Internet is much more susceptible to deliberate attacks of removing the AS's with highest degree than previous studies that did not take into consideration BGP polices.

Hu et. al [7] also investigate logical failures on an AS-level graph, focusing opportunities to limit the impact of logical failures. Like us, they augmented thair AS graph with IXP connectivity data. Unlike our work, they did not use this data to consider the possibility of correlated failures. Rather, they investigated using IXPs to provide backup peers to improve connectivity in case of emergency.

Outage Events. Real outage events highlight the threat of correlated failure in geographic locations which suffer disaster or attack. For example, the 2006 Boxing Day Earthquake in Taiwan resulted in major Internet outages when six of seven undersea cables connecting North and Southeast Asia with eachother and North America disconnected [6]. While the earthquake did not cause complete disconnectivity, the affected networks suffered heavy congestion until the cables were repaired. This experience serves already as a case study for emergency restoration in case of disaster [8].

[**justine: agreed wrt the 2003 study, doesn't look as relevant as the Taiwan quake**]

PoP-level Internet Topologies. Our model for network connectivity focuses on *failure points*, physical locations where multiple networks connect, leading to multiple correlated failures in case of disaster. We borrow techniques and data for discovering these physical locations from iPlane [9] and the IXP Mapping Project [4]. iPlane clusters IP addresses into PoPs using a combination of DNS-based geolocation and TTL-based distance measurements. The IXP Mapping project uses public IXP membership datasets, DNS names, looking glass servers, BGP tables, active traceroute and ping measurements, and other sources to provide the most accurate IXP membership datasets available to date.

Network Security Policy.

- White House POlicy Review [2]

6. CONCLUSION

[**restate what we did and what we found**] [**our conclusions: network operators need not just logical but physical redundancy - diversity of location. also, tradeoff between efficient exchange in IXPs (getting lots of people to same place) and creating a juicy target. thus we should really really secure these places!**]

7. REFERENCES

[1] USA Patriot Act. H.R. 3162, Public Law 107-56.

[2] USA White House Cyberspace policy review. `http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf`, 2009.

[3] R. Albert, H. Jeong, and A.-L. Barabasai. Error and attack tolerance of complex networks. *Nature*, July 2000.

[4] B. Augustin, B. Krishnamurthy, and W. Willinger. IXPs: mapped? In *IMC*, 2009.

[5] D. Dolev, S. Jamin, O. O. Mokryn, and Y. Shavitt. Internet resiliency to attacks and failures under bgp policy routing. *Computer Networks*, 50(16):3183 – 3196, 2006.

[6] D. Greenlees and W. Arnold. Asia scrambles to restore communications after quake. The New York Times, December 28 2006.

[7] C. Hu, K. Chen, Y. Chen, and B. Liu. Evaluating potential routing diversity for Internet failure recovery. In *INFOCOM*, 2010.

[8] Y. Kitamura, Y. Lee, R. Sakiyama, and K. Okamura. Experience with restoration of asia pacific network failures from taiwan earthquake. *IEICE ToC*, November 2007.

[9] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: an information plane for distributed services. In *OSDI*, 2006.

[10] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang. The (in)completeness of the observed Internet AS-level structure. *IEEE/ACM ToN*, February 2010.

[11] M. Omer, R. Nilchiani, and A. Mostashari. Measuring the resilience of the global Internet infrastructure system. In *IEEE International Systems Conference*, 2009.

[12] J. Wu, Y. Zhang, Z. M. Mao, and K. G. Shin. Internet routing resilience to failures: analysis and implications. In *CoNEXT*, 2007.