Studying the Importance of Content Providers on Internet Robustness Metrics

Ivana Bachmann
NIC Labs, Universidad de Chile, Chile
ivana@niclabs.cl
Fernando Morales
NIC Labs, Universidad de Chile, Chile
fernando@niclabs.cl
Javier Bustos-Jiménez
NIC Labs, Universidad de Chile, Chile
jbustos@niclabs.cl
Alonso Silva
Bell Labs, Nokia, Francia
alonso.silva@nokia-bell-labs.com

Abstract

Whether as telecommunications or power systems, networks are very important in everyday life. Maintaining these networks properly functional and connected, even under attacks or failures, is of special concern. This topic has been previously studied with a *whole network robustness perspective*. This perspective measures the average behavior of the network after its last node has failed.

Here, we propose an alternative to well-known studies about the robustness of the backbone Internet: to use a supply network model and the supply availability ratio as metric. Our research question is: if a smart adversary has a limited number of strikes to attack the Internet, how much will the damage be after each one in terms of network supplying?

1 Introducción

Redes como la red eléctrica, de transporte y telecomunicaciones, por nombrar algunas, se han vuelto fundamentales para que el mundo moderno se mantenga en funcionamiento. Por ello mantener estos sistemas operando correctamente es de gran importancia. Sin embargo estos sistemas son propensos a fallos, ya sea por mal funcionamiento del sistema o ataques a este. Estas estructuras han sido estudiadas como redes complejas donde sus componentes se representan como nodos y las relaciones entre dichas componentes como arcos.

Dado que el buen funcionamiento de estos sistemas requiere que la red se encuentre bien conectada es de suma importancia estudiar su capacidad para resistir fallos, ya sean estos accidentales o planeados. Esta capacidad es llamada robustez.

Cabe preguntarse entonces qué significa que una red se encuentre bien conectada. Para responder esta pregunta primero se debe identificar cómo funciona la red. En el caso de la red de Internet se tienen usuarios que consumen contenido ya sea a través de un navegador o alguna aplicación. Para ambas situaciones el usuario debe ser capaz de contactarse con el proveedor de contenidos. Si los usuarios no pueden consumir contenidos los podemos considerar como desconectados de Internet. Luego para el caso de la red de Internet esta está bien conectada si los usuarios son capaces de comunicarse con el o los proveedores de contenido.

En este trabajo nos enfocamos en el caso de ataques intencionales ejecutados por un adversario para una red que posee proveedores y consumidores. Para lograr esto se considera como métrica de robustez una métrica que considera la existencia de un proveedor. Se puede observar que el caso de ataques intencionales corresponde a una cota superior en el daño que se puede inflingir a la red.

Consideramos que un adversario debería utilizar una estrategia *greedy* o glotona, apuntando a maximizar el daño con el menor número de ataques. Así, en este artículo se discute el desempeño de ataques sobre el Backbone de Internet (la red formada por puntos de intermabio de Internet, IXP) y su correlación con lo que los usuarios de Internet perciben si lo que ellos desean es consumir contenido desde (Google), el mayor proveedor de contenido. Para ello se utiliza como primera aproximación el Supply Availability Ra-

 This work was partially funded by CORFO 15BPE-47225: "Estudio y recomendaciones sobre la resiliencia de la infraestructura del internet chileno".

tio (SAR) donde el proveedor es Google.

La idea de considerar una red basada en IXP como "El Backbone de Internet" no es nueva, esta ha sido previamente utilizada como parte del "core de Internet" para estudiar los patrones de tráfico entre SAs (sistemas autónomos) y una evolución entre estrategias de provider peering [LIJM+11], para optimizar la entrega de contenido de Google a través de caminos directos [CSR+15] y en el Internet Backbone Market [BFBS05]. Nuestro estudio es novedoso por el uso de la red de IXP como un modelo para "El Backbone de Intenet", el cual nos puede dar una aproximación de la estructura física de Internet, y por considerarla como una red de suministro para estudiar su robustez. Hasta donde los autores tienen conocimiento, esta es la primera vez que la robustez de la red IXP es estudiada.

El artículo se organiza de la siguiente forma: la siguiente sección presenta trabajo relacionado, seguido por la metodología para crear la red IXP, la estrategia de ataque usando SAR (Sección 4). Las conclusiones son presentadas en la sección 5.

2 Trabajo relacionado

Para estudiar la robustez de una red, su evolución ante fallos debe ser analizada. En situaciones del mundo real las redes pueden enfrentarse tanto a fallas aleatorias como ataques intencionales. Para esta última dos categorías principales de estrategias de ataque han sido definidas: ataques simultáneos y ataques secuenciales [HKYH02a]. Los ataques secuenciales sobre enlaces eligen un enlace a remover y dado el impacto de su remoción sobre la red, elige el siguiente. Este proceso continúa iterativamente hasta remover el número de enlaces deseado. El caso de nodos es análogo.

Los ataques secuenciales han sido estudiados a fondo para analizar la robustez en redes. Holme et al. probó estrategias de ataques simultáneos y secuenciales usando medidas de centralidad como grado y betweenness.

Betweenness [BMSBJ12] es una métrica que determina la importancia de un arco de acuerdo a la cantidad de caminos mínimos que pasan a través de él. Betweenness ha sido estudiada como métrica de robustez para la capa de ruteo [SHS+11], como métrica de robustez para redes complejas [IKSW13] y para redes de sistemas autónomos de Internet [MKF+06], entre otros. Betweenness ha sido ampliamente estudiado y estandarizado como base de comparación para métricas de robustez. Por estas razones en este estudio será utilizada para comparar desempeño.

Más recientemente [VA15] estudió ataques secuenciales multi-estrategia usando múltiples medidas de robustez, incluyendo la *Unique Robustness Measure* o *Medida Única de Robustez* (R-index) [SMA+11].

En [BRSBJ15] los autores presentan valores parciales del R-index a medida que los nodos son desconectados, mostrando la importancia de escoger una métrica de robustez apropiada para realizar los ataques.

Para entender mejor el tema de ataques a redes y estrategias, ver [HKYH02b, MR06, RW10, SSYS10].

3 Construyendo el grafo del backbone de Internet

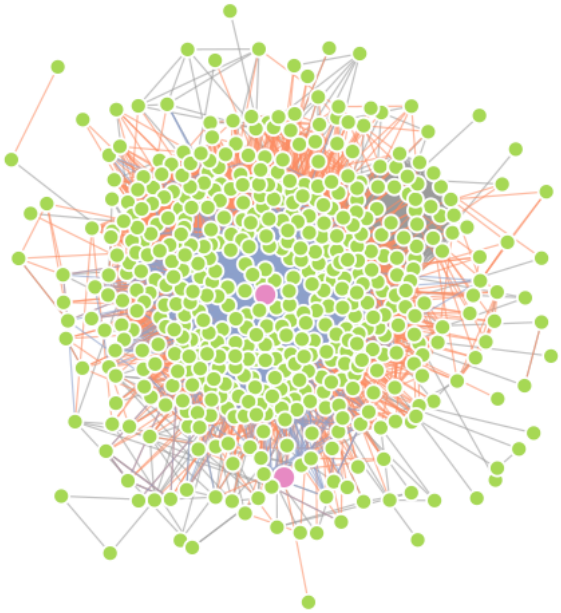

Figure 1: Grafo de Peering

Dentro de Internet, peering corresponde al contrato entre dos sistemas autónomos (SAs) que acuerdan intercambiar rutas de tráfico a través de un enlace físico. [DD10] presenta que el core de Internet es una jerarquía multi-tier de proveedores de tránsito (Transit Providers o TPs) donde aproximadamente 10-20 de los tier-1 TPs, presentes en muchas regiones geográficas, están conectadas a un clique de enlaces de peering. Los ISPs (tier-2) son consumidores de los TPs de tier-1 y a su vez los proveedores de residencias o pequeñas empresas (tier-3) corresponden a los TPs de tier-2.

A través de `peeringdb.com` recolectamos los sistemas autónomos de cada Punto de Intercambio de Internet (Internet Exchange Point, IXP) y los definimos como nodos del grafo. De esta forma un SA podría pertenecer a diferentes IXPs y un IXP podría tener múltiples SAs. Luego, conectamos los nodos mediante un arco si cumplen al menos una de las siguientes reglas: SAs conectados físicamente que intercambian tráfico, SAs que pertenecen a un mismo IXP, SAs que pertenecen a una misma instalación.

Donde los IXP son considerados como peering público y las intalaciones como peering privado.

La figura 1 muestra el grafo resultante, este tiene 522 nodos y 14.294 arcos (los arcos naranjos representan peering público, los arcos azules peering privado y los verdes conexión directa por red). La red resultante tiene un core bien conectado con algunos nodos aislados en su borde.

4 Ratio de Disponibilidad de Suministro (Supply Availability Ratio)

En 2013 se reportó que que Google poseía el 40% del tráfico de Internet[1]. En consecuencia, dada las políticas de peering de Google[2] y sus políticas para interconectar datacenters [JKM+13], podemos estudiar Internet como una red de suministro adaptando la métrica SAR presentada en [ZKY11].

1. **Supply Availability Ratio** (SAR): Porcentaje de sistemas autónomos que tiene acceso a Google a través de al menos uno de sus SAs.

Cabe observar que Google ha delegado algunos servicios a sistemas autónomos de ISPs [CFH+13], sin embargo éstos eventualmente deben conectarse con el backbone de Google para actualizarse.

Utilizando una estrategia de ataque basada en betweenness (ver trabajo relacionado) calculamos SAR para distintos porcentajes de arcos removidos. Los resultados son presentados en la Figura 2.

El Ratio de Disponibilidad de Suministro presenta una alta relación con el tamaño fraccional de la componente conexa más grande, la cual, en este estudio, incluye al menos un SA de los dos SAs presentes de Google (marcados en rosado en le figura 1, AS15169 en el centro de la red y AS36040 en la orilla de la red).

Se debe notar que para un usuario dentro del core de la red el principal proveedor de contenidos siempre existe y por lo tanto, para él, no hay indicios de que la red se esté desarmando (o perdiendo a la mitad de sus miembros como es el caso luego de remover 20% de sus arcos). Sin embargo la realidad es otra: luego de desconectar solo un 5% de la red uno de los SAs de Google queda aislado, mostrando que en este punto la red está siendo mantenida únicamente por AS15169.

5 Conclusiones y trabajo futuro

En este artículo hemos presentado qué tan robusto sería el backbone de Internet (la red de SAs de peering) si un adversario escogiera sabiamente que enlace va a cortar. Siguiendo recomendaciones, el enlace elegido sería aquel con mayor betweenness.

[1] Ver el artículo de Forbes en `http://goo.gl/aHdeiN`

[2] Ver `https://peering.google.com/#/options/peering`.

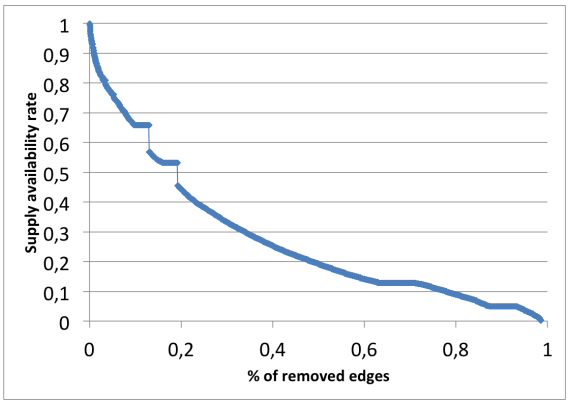

Figure 2: Supply Availability Ratio o Ratio de Disponibilidad de Suministro

Con esta estrategia el adversario es capaz de desconectar la mitad de la red removiendo apenas un 20% de los arcos, más de un 30% de los nodos luego de remover un 10% de los arcos y un 10% de los nodos luego de remover un 1% de los arcos.

Además, hemos considerado Internet como una red de suministro donde Google es el principal proveedor de contenido y proponemos estudiar la robustez del backbone de Internet a través del Supply Availability Ratio (SAR). Dado que en nuestro contexto SAR se define como el porcentaje de sistemas autónomos que tiene acceso a Google a través de al menos uno de sus SAs, SAR presenta gran concordancia con el tamaño fraccional de la componente conexa más grande pues dicha componente siempre posee un SA de Google y, por lo tanto, los nodos de la componente conexa más grande siempre tienen acceso a google.

Como trabajo futuro se planea extender el uso de medidas de suministro que consideren otros parámetros de la red, de forma de obtener una visión completa del estado de la red.

References

[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 *International Conference of the Chilean Com-*

puter Science Society, pages 1–6, Nov 2015.

[CFH+13] Matt Calder, Xun Fan, Zi Hu, Ethan Katz-Bassett, John Heidemann, and Ramesh Govindan. Mapping the expansion of google's serving infrastructure. In *Proceedings of Internet Measurement Conference*, pages 313–326. ACM, 2013.

[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 CoNEXT*, pages 21:1–21:12, New York, NY, USA, 2010. ACM.

[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.

[JKM+13] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, et al. B4: Experience with a globally-deployed software defined wan. *ACM SIGCOMM Computer Communication Review*, 43(4):3–14, 2013.

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

[MKF+06] Priya Mahadevan, Dmitri Krioukov, Marina Fomenkov, Xenofontas Dimitropoulos, Amin Vahdat, et al. The internet as-level topology: three data sources and one definitive metric. *ACM SIGCOMM Computer Communication Review*, 36(1):17–26, 2006.

[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 *Ultra Modern Telecommunications and Control Systems and Workshops*, pages 497–503. IEEE, 2010.

[SHS+11] Paul Smith, David Hutchison, James PG Sterbenz, Marcus Scholler, Ali Fessi, Merkouris Karaliopoulos, Chidung Lac, and Bernhard Plattner. Network resilience: a systematic approach. *Communications Magazine, IEEE*, 49(7):88–97, 2011.

[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.

[VA15] Mario Ventresca and Dionne Aleman. Network robustness versus multi-strategy sequential attack. *Journal of Complex Networks*, 3(1):126–146, 2015.

[ZKY11] Kang Zhao, Akhil Kumar, and John Yen. Achieving high robustness in supply distribution networks by rewiring. *Engineering Management, IEEE Transactions on*, 58(2):347–362, 2011.