

EL CORTE DE SHAKARIAN

La Real Academia Española define resiliencia como:

- 1.- Capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.
- 2.- Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

Cuando llevamos este término a Internet y las redes de comunicaciones, ¿qué se entiende cuando hablamos de resiliencia?, específicamente, ¿qué se entiende como una red resiliente?



IVANA BACHMANN

Estudiante de Magíster en Ciencias mención Computación, Departamento de Ciencias de la Computación, Universidad de Chile (DCC). Asistente de Investigación NIC Labs. Líneas de investigación: Redes Interdependientes, resiliencia en redes.

ivana@niclabs.cl



JAVIER BUSTOS

Director de NIC Labs, laboratorio de investigación de NIC Chile. Profesor Adjunto del Departamento de Ciencias de la Computación (DCC), Universidad de Chile. Doctor en Informática, Universidad de Niza Sophia-Antipolis, Francia. Líneas de investigación: Redes, Sistemas Distribuidos, Dispositivos Móviles.

jbustos@niclabs.cl

Tal vez usted pensó en la capacidad que tiene la red para soportar la caída de alguno de sus componentes, eso es tolerancia a fallas. Entonces pensó en una medida de qué tan buena es la red para soportar esas caídas, esa son métricas de robustez. ¿Cuánto toma en arreglarse el servicio? Eso se define en un *Service Level Agreement* (SLA). ¿Cuántas caídas soporta la red antes de colapsar? Esas son métricas de percolación.

Entonces ¿qué se entiende como resiliencia de redes? Es una mezcla de todo lo anterior: métricas de tolerancia a fallas, estimación de pérdida por falla de una componente, estimación de tiempos y causas de percolación, órdenes de magnitud de pérdida que produce la falla, y estimaciones de tiempo de recuperación. En redes complejas, como el Internet actual, es un tema bastante difícil (y por lo tanto interesante) de estudiar.

Desde el punto de vista más simple se puede tomar a Internet como una red de dos dimen-

siones: la física (cables, fibra, etc.) y la lógica, representada por ejemplo por la red resultante del protocolo BGP¹, donde los ISPs intercambian la información de sus rutas mediante el uso de Sistemas Autónomos (conocidos por su sigla AS en inglés). Por lo tanto, la topología de Internet se puede considerar como un grafo de conexión de sistemas autónomos conectados mediante enlaces virtuales

Estudiar la resiliencia de únicamente la capa lógica o únicamente la capa física, permite comprender el comportamiento de cada capa por separado frente a potenciales amenazas. Sin embargo, este tipo de estudios no toma en cuenta que ambas capas no existen de forma aislada, sino que interactúan entre sí y pueden relacionarse de manera que los cambios en una capa pueden afectar a la otra. Los estudios de métricas de resiliencia en este tipo de redes (grafos) unidimensionales se han estudiado largamente por su uso en todo tipo de red compleja (transporte, redes sociales, etc.), y en general se comparan

¹ https://es.wikipedia.org/wiki/Border_Gateway_Protocol

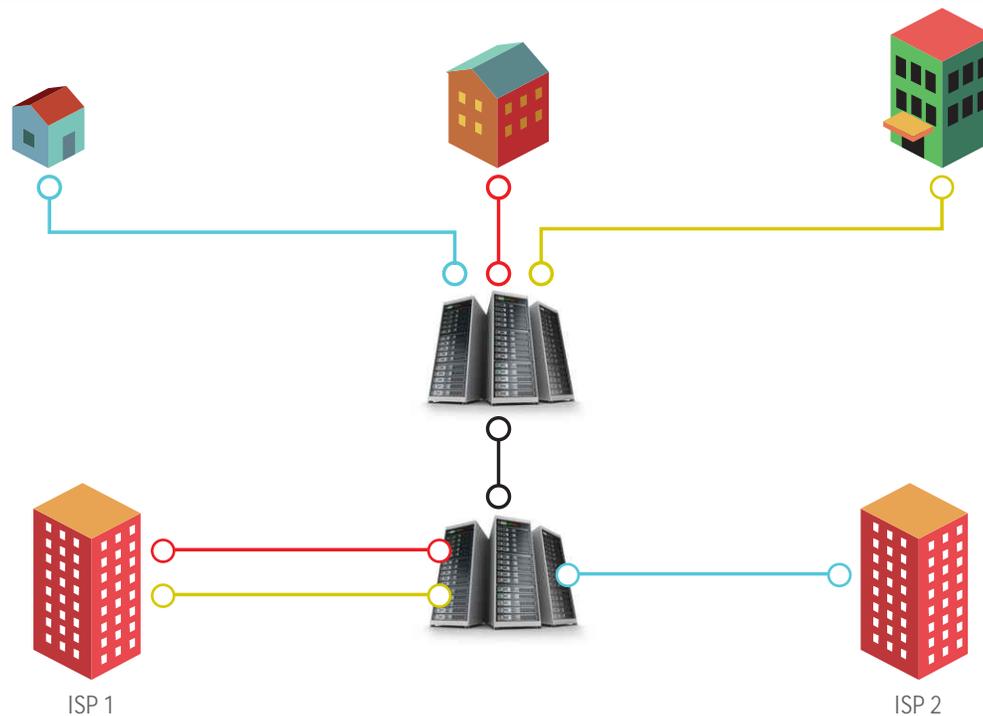


FIGURA 3. LA RED DE LOS PROVEEDORES DE INTERNET Y SUS CIRCUITOS LÓGICOS PASAN POR LA MISMA FIBRA ÓPTICA QUE CONECTA LOS ROUTERS (COLOR NEGRO).

Otro enfoque, presentado como un ataque mejorado a la red [6,7], es volver a calcular *betweenness* después de la eliminación de cada nodo. Estudios en profundidad de esas estrategias, como [8,9], muestran un impacto similar de estrategias que no recalculan descartando a veces solo la mitad de los nodos equivalentes.

REDES INTERCONECTADAS

Si pensamos en cada capa de Internet como una red de enlaces y nodos, donde los nodos son puntos de conexión o servidores y los enlaces son cables o conexiones lógicas entre servidores, dependiendo de la capa o dimensión que se está observando se puede apreciar que, por ejemplo, muchos cables pueden estar pasando por exactamente un mismo lugar, o la

comunicación pasar por la misma fibra (recordar que Internet es una red basada en comunicación de paquetes). Sin embargo, en el nivel lógico estas conexiones se ven como conexiones disjuntas, distinguibles entre sí. En la Figura 3 se muestra este fenómeno. Entonces, un corte de cable puede afectar muchos enlaces “lógicos”.

¿Puede esto suceder? En el año 2010, un terremoto de 8.8Mw sacudió a Chile central tirando por tierra algunos puentes cuya estructura soportaba las líneas de fibra óptica de distintos ISPs chilenos, y dejando sin Internet al país por casi un día [10]. Otro ejemplo sucedió en 2011, cuando una mujer de 75 años llamada Hayastan Shakarian (Imagen 1), quien buscaba metales en el límite entre Georgia y Armenia, cortó una fibra del Georgian Railway Telecom dejando sin Internet al 90% de los usuarios privados y corporativos de esa firma en Armenia por alrededor de 12 horas.

Hemos visto ejemplos de que cuando ocurre una desconexión a nivel físico, por ejemplo cuando se cortan los cables de comunicación, esta desconexión tiene efectos inmediatos sobre las conexiones en el nivel lógico las que pueden verse de una forma completamente distinta de una capa a otra. Para enfrentar esto se ha planteado modelar matemáticamente las relaciones entre ambas capas, donde la relación sea capaz de transmitir los efectos de un eventual ataque o falla.

En cuanto al modelamiento de ataques en redes interdependientes, en [11] se analiza un modelo de dependencia uno a uno entre nodos de redes con igual distribución, y se obtienen datos teóricos respecto al umbral de percolación sobre el modelo desarrollado mostrando que las redes interdependientes se comportan de forma sumamente diferente, incluso opuesta, a las redes unitarias. En este artículo se analizan ataques a nodos y se estudia el daño que causan a las redes

participantes. Para dos redes interdependientes, la desconexión de un nodo en una red causa la desconexión del nodo de la otra red con la cual está conectado, provocando una serie de desconexiones en cascada hasta converger a un estado en que las ya no se puede seguir desconectando nodos.

En [12] se realiza una generalización del modelo presentado en [11] a dos o más redes que pueden interactuar, ya sea uno a uno entre nodos de distintas redes, uno a muchos, o bien a través de dependencias dirigidas, en la que la dependencia de un nodo a con un nodo b no necesariamente significa que el nodo b dependa del nodo a . Para obtener resultados teóricos, estos modelos toman como supuesto que la distribución de las redes participantes es la misma y que las conexiones entre redes siguen estructuras bien definidas. En [13] se continúa sobre las bases sentadas en [11] respecto a redes interdependientes y se estudia la robustez de este tipo de redes bajo ataque a los nodos interdependientes.

Además de estos modelos, en [14] se ofrece una recopilación de trabajos sobre modelamiento de redes interdependientes y se muestra un rediseño de estos con el objetivo de generalizar los modelos existentes. Primero se presenta un modelo multicapa, donde se tienen capas compuestas por capas elementales, en la que los nodos de la red pueden existir en una o más capas a la vez y establecer conexiones con nodos de la misma capa o de capas distintas. Luego se presenta un modelo de coloreo de nodos, el cual corresponde a la representación de un caso particular del modelo de capas donde un mismo nodo puede pertenecer sólo a una capa.

Con estos modelos las redes interdependientes presentadas en [11,12,13] se pueden modelar como las capas de una misma red. Además, es posible modelar redes que no necesariamente corresponden a redes distintas interdependientes, sino que corresponden a una misma red con diferentes representaciones de sí misma.



IMAGEN 1.
HAYASTAN SHAKARIAN (FOTO DE AFP).

EN CHILE

En nuestro país, más precisamente en la Universidad de Chile, los profesores José Miguel Piquer

y Javier Bustos se adjudicaron (en conjunto con SUBTEL) el proyecto CORFO 15BPE-47225: “Estudio y recomendaciones sobre la resiliencia de la infraestructura del Internet chileno”, este programa es desarrollado con aportes del Fondo de Inversión Estratégica, del Ministerio de Eco-

nomía, Fomento y Turismo. A partir de enero de 2016 se realizará una radiografía del Internet chileno, y se buscará estudiar y medir la red de datos chilena para poder hacerla más resiliente ante emergencias, catástrofes o ataques. ■

REFERENCIAS

- [1] P. Smith, D. Hutchison, J. P. Sterbenz, M. Scholler, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner. Network resilience: a systematic approach. *Communications Magazine, IEEE*, 49(7):88–97, 2011.
- [2] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang. Attack robustness and centrality of complex networks. *PloS one*, 8(4):e59613, 2013.
- [3] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, A. 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.
- [4] J.P. Sterbenz, E.K. Cetinkaya, M. Hameed, A. Jabbar, J.P. Rohrer, et al. Modelling and analysis of network resilience. In *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, pages 1–10. IEEE, 2011.
- [5] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. Sterbenz. Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach. *Telecommunication Systems*, 52(2):751–766, 2013.
- [6] J. Rak and K. Walkowiak. Survivability of any-cast and unicast flows under attacks on networks. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pages 497–503. IEEE, 2010.
- [7] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm. Characterising the robustness of complex networks. *International Journal of Internet Technology and Secured Transactions*, 2(3-4):291–320, 2010.
- [8] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.
- [9] W. Molisz and J. Rak. End-to-end service survivability under attacks on networks. *Journal of Telecommunications and Information Technology*, pages 19–26, 2006.
- [10] V. Ramiro, J. Piquer, T. Barros and P. Sepúlveda. The Chilean Internet: Did It Survive The Earthquake? *WIT Transactions on State-of-the-art in Science and Engineering*, vol 18, pages 19, 2012.
- [11] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, Apr. 2010.
- [12] J. Gao, S. V. Buldyrev, H. E. Stanley, X. Xu, and S. Havlin. Percolation of a general network of networks. *Physical Review E*, 88:062816+, Dec. 2013.
- [13] S. Shai, D. Y. Kenett, Y. N. Kenett, M. Faust, S. Dobson, and S. Havlin. Resilience of modular complex networks. *CoRR*, abs/1404.4748, 2014.
- [14] M. Kivela, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter. Multilayer networks. *Journal of Complex Networks*, 2(3):203–271, Sept. 2014.