Detección de Enlaces Intercontinentales

Manuel Costa Mathias Gatti

Resumen —

Index Terms —**traceroute, enlaces intercontinentales, ICMP, anomalías, RTT, TTL**

I. Introducción

Este trabajo gira en torno al funcionamiento y aplicación de traceroute, una herramienta que permite analizar y seguir la traza de los distintos nodos por los que pasa un paquete cuando intenta alcanzar cierto host destino. Para conseguir el mejor entendimiento de la herramienta, realizaremos nuestra propia implementación.

Utilizando métricas como la latencia de red en conjunto con la ubicación de las IPs de los hops intentaremos aprender sobre los caminos que realizan los paquetes de internet y los tiempos que estos manejan. Finalmente implementaremos y evaluaremos un método para detectar automáticamente enlaces continentales a partir de un análisis estadístico de los Round Trip Times (RTT).

A lo largo de este informe describiremos los detalles de la implementación realizada, los resultados obtenidos y sus limitaciones.

II. Métodos

Herramientas

Para la implementación de traceroute utilizamos el código provisto por la cátedra al cual le realizamos ciertas modificaciones para poder detectar anomalías y guardar los datos obtenidos de forma más cómoda.

Detección de saltos intercontinentales

Para la detección automática de saltos intercontinentales aplicamos una técnica basada en el Modified Thompson Tau Test para detección de outliers, como se explica en [Cimbala][1]. Dicho test consiste en comparar el valor absoluto de las muestras estandarizadas (mediante z-score) contra un estadístico, τ, que depende del tamaño de la muestra. En particular, nuestra versión difiere con la presentada en [Cimbala] en que no tomamos el valor absoluto del z-score, dado que no estamos interesados en detectar los casos atípicamente pequeños.

Asunciones realizadas

- A los fines prácticos, vamos a considerar que un salto de América del Sur a América del Norte se considera un salto intercontinental, por la extensión del mismo.
- A veces se da el caso en que el RTT promedio para un cierto TTL puede ser menor que el RTT del TTL anterior. Ante esta situación seteamos el RTT diferencial (delta) en 0. Razones por las que puede suceder esto son el problema de los *caminos asimétricos*, o bien que haya un desvío estándar elevado y el hop realizado sea corto. O sea que este 0 no debe ser considerado como que realmente el tiempo de RTT es despreciable, si no más bien como un resultado desafortunado. Se nos presentó entonces la duda de si considerar estos valores o no a la hora de hacer el cálculo de los *outliers*. Basados en la observación empírica de que el *false positive rate* para el método de Cimbala era cercano a 1 cuando dejábamos los 0s, decidimos excluirlos (básicamente sucedía que casi cualquier valor distinto a 0 era considerado un outlier). Esta decisión ciertamente está acoplado al set de sites que escogimos, pero consideramos que es una medida razonable en cualquier caso.

Rutas

Se corrió traceroute sobre 3 universidades distintas con un ttl de 30 y 40 queries. Con el objetivo de lograr contrastar elegimos universidades muy lejanas y muy cercanas. A continuación describimos brevemente a cada una.

- Universidad de São Paulo (`www5.usp.br`) esta será la universidad mas cercana, ubicada en el mismo continente, por lo cual esperamos que no haya ningún enlace intercontinental.
- Universidad de Sidney (`www.sydney.edu.au`) escogimos esta universidad ya que nos surgió la duda de si existirá algún enlace intercontinental directo entre Oceanía y América o tendrá que pasar europa resultando en varios enlaces.
- Universidad de Moscú (`www.msu.ru`) al estar ubicada en un punto tan alejado de nosotros estábamos seguros de que iba a haber algún salto intercontinental y quizás más.

III. Resultados y análisis

Los resultados de cada ruta se presentan en dos partes: primero se realiza una descripción geográfica de la ruta trazada, basada en las ips seguidas, prestando particular atención a los saltos intercontinentales; en la segunda parte se analizan los RTTs entre saltos, de los cuales se busca poder inferir en forma automática los enlaces intercontinentales detectados en la primer parte.

M. Costa, e-mail: manucos94@gmail.com
M. Gatti, e-mail: mathigatti@gmail.com

[1] http://www.mne.psu.edu/cimbala/me345/Lectures/Outliers.pdf

Universidad de São Paulo

Recorrido en el Planisferio

A continuación se puede ver el recorrido realizado por los paquetes enviados al destino. Como era de esperarse no se realizan saltos intercontinentales, si no que se forma un camino bastante directo de Buenos Aires a São Paulo.

De los 13 saltos necesarios para llegar al destino, 4 no respondieron el TTL, resultando en un 30 % de saltos sin respuesta de *time exceeded* y un largo de ruta de 9 hops que si respondieron.

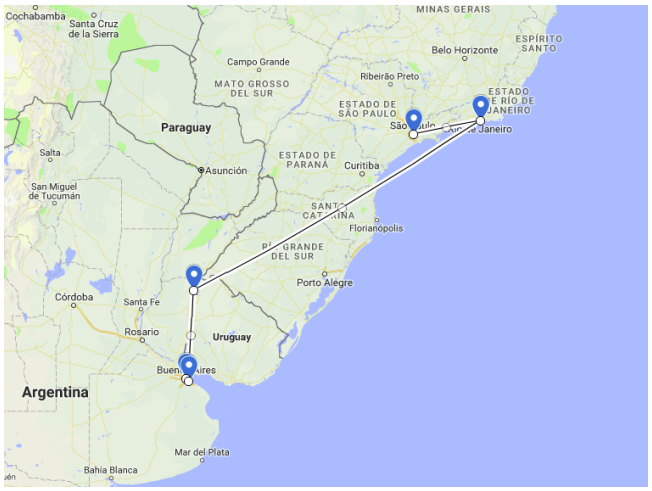

Figura 1: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio `www5.usp.br`

RTT entre saltos

Analicemos cómo funciona nuestro modelo para inferir saltos intercontinentales, en un caso donde sabemos que no hay ninguno.

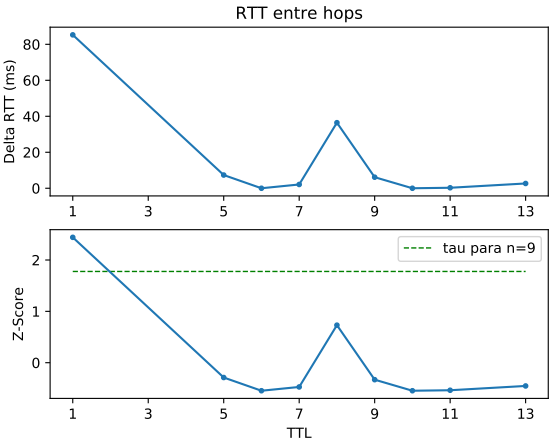

Figura 2: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio `www5.usp.br`. n es la cantidad de TTLs para los que se obtuvo un *time exceeded* (que son los puntos que se grafican).

Los outliers detectados por el método de Cimbala son los siguientes (en este orden):

- Salto 1 con z-score 2.08151529601 ($n = 7$)
- Salto 8 con z-score 2.00270114286 ($n = 6$)

Obviamente, ambos son falsos positivos. Podemos entender esto como una consecuencia de que el test utilizado no hace más que buscar valores atípicos (en nuestro caso atípicamente grandes) dentro de una muestra. Por lo tanto, en la medida que los RTTs entre hops no sean equitativos, no es de sorprender que casi siempre encontremos algún salto que sobresalga del resto. La clave está en que si tuviéramos un trayecto significativamente más largo, este valor que ahora resulta un outlier muy posiblemente quedaría opacado por el RTT diferencial de un verdadero salto continental. Esto es más claro para el segundo outlier, que coincide con el salto de Argentina a Brasil (un salto relativamente grande para esta muestra, ver figura 2).

Vale decir que en el primer caso lo que parece estar sucediendo es que hay una cuestión técnica de la LAN desde la cual se dispara el *traceroute* que dificulta alcanzar el *gateway*, pues 80ms parece un tiempo elevado para esto (viendo la figura 2 el RTT de este hop supera por mucho al que va hasta Río de Janeiro).

Universidad de Moscú

Recorrido en el Planisferio

A continuación se puede ver el recorrido realizado por los paquetes enviados al destino, este en principio puede ser extraño ya que realiza 3 saltos intercontinentales, en vez de 1 o 2 como era de esperarse, más adelante nos explayaremos un poco sobre las razones por las cuales pudo haber sucedido esto.

De los 30 saltos necesarios para llegar al destino 3 no respondieron el TTL, resultando en un 10 % de saltos sin respuesta de time exceeded y un largo de ruta de 27 hops que si respondieron.

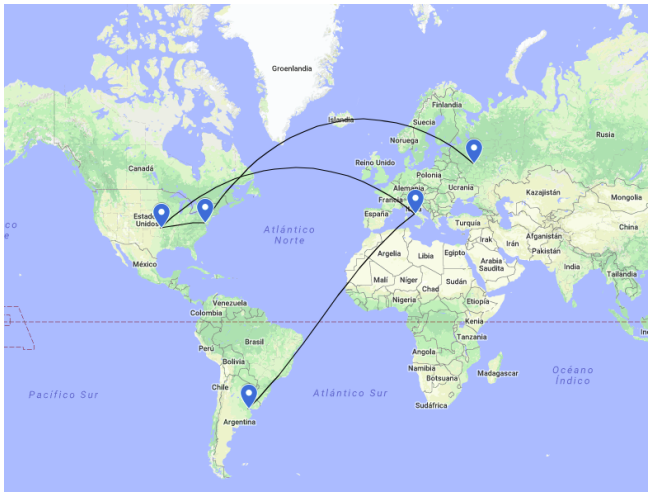

Figura 3: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio `www.msu.com`

RTT entre saltos

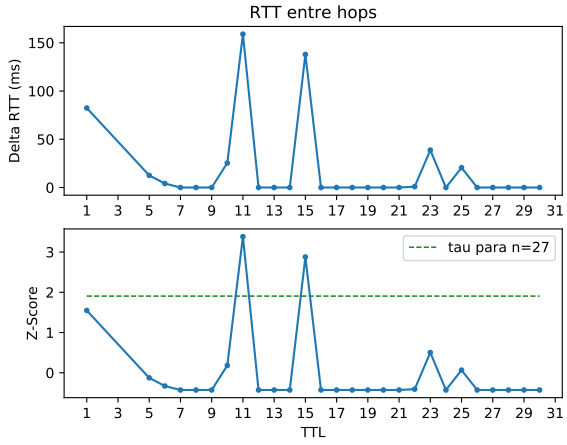

Figura 4: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio `www.msu.com`. n es la cantidad de TTLs para los que se obtuvo un *time exceeded* (que son los puntos que se grafican).

Para este sitio, el algoritmo detecta los siguientes enlaces continentales:

- Salto 11 con z-score 1.78130453282 ($n = 9$)
- Salto 15 con z-score 2.07044455379 ($n = 8$)
- Salto 1 con z-score 2.00892644697 ($n = 7$)

Este caso tiene bastantes particularidades, relacionadas con la ruta compleja que se observó en el punto anterior.

El primer outlier, que se da en el salto 11, coincide con un salto a un router de Roma, Italia (`89.221.41.171`). La cuestión es que el nodo desde el cual se realiza el hop también está ubicado en Italia (`185.70.203.32`), y dicho salto no fue detectado como outlier, pues en efecto tiene un RTT mucho más bajo. Una posible hipótesis que manejamos al respecto de porqué ocurrió esto (que no se detecte el salto continental, pero sí el siguiente hop) es que el primer router al que se llega sea uno de los principales gateways de Italia, lo que provoque que se encuentre congestionado y el paquete que se manda quede encolado un largo tiempo antes de forwardearse al siguiente hop.

El segundo punto atípico, con TTL 15, presenta una situación similar: el destino está en Estados Unidos, pero los tres saltos anteriores también, y no fueron detectados. Acá hay una diferencia sin embargo: esos tres saltos mostraron todos RTTs diferenciales de 0, lo que implica que de hecho el RTT promedio de estos nodos fue menor que el promedio del último router que estaba en Italia. Este parece ser un caso de *camino asimétrico* (Jobst 2012). Razonablemente existe una mejor ruta desde Estados Unidos a Argentina, que cruzar toda Europa. Que la ruta no haya ido directamente por Estados Unidos, salteandose Italia, suena a una consecuencia de un cambio del estado de la red: posiblemente el paquete se mandó a Italia porque había una ruta aprendida que iba directamente de Italia a Rusia sin salir del continente, pero por alguna razón dicho camino *óptimo* dejó de estar habilitado.

Nuevamente se detectó el primer salto, dado que este experimento fue corrido desde la misma LAN.

En definitiva, hay que decir que en este caso tuvimos tres falsos positivos y tres falsos negativos (Argentina-Italia, Italia-USA, USA-Rusia).

Universidad de Sidney

Recorrido en el Planisferio

A continuación se puede ver el recorrido realizado por los paquetes enviados a Sidney, se realizaron 2 saltos intercontinentales. Uno de Argentina a Estados Unidos y otro de Estados Unidos a Australia lo cual parece indicar que no hay una conexión directa de América del Sur a oceanía pero si desde América del Norte.

De los 26 saltos necesarios para llegar al destino 6 no respondieron el TTL, resultando en un 23 % de saltos sin respuesta de time exceeded y un largo de ruta de 20 hops que sí respondieron.

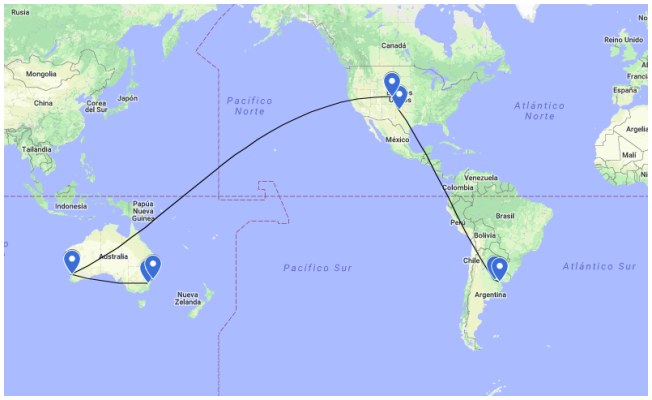

Figura 5: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio `sydney.edu.au`

RTT entre saltos

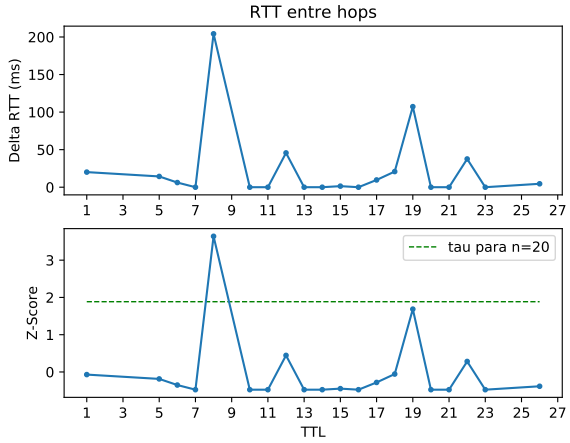

Figura 6: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio `sydney.edu.au`. n es la cantidad de TTLs para los que se obtuvo un *time exceeded* (que son los puntos que se grafican).

Los resultados arrojados por el algoritmo fueron:

- Salto 8 con z-score 2.62854380167 ($n = 11$)
- Salto 19 con z-score 2.540003618 ($n = 10$)
- Salto 12 con z-score 1.83643437065 ($n = 9$)
- Salto 22 con z-score 1.97868824766 ($n = 8$)

Para esta ruta vemos que se detectó un salto intercontinental en el octavo hop. Este efectivamente fue un salto de Argentina a Estados Unidos (que como mencionamos en la sección anterior, vamos a considerar un salto continental). Asimismo, se detectó el salto de Estados Unidos a Australia (TTL 19).

Sin embargo tuvimos dos falsos positivos también: tanto el salto 12 como el 22 fueron detectados aunque no son saltos continentales. De todas formas hay que destacar que el hop 22 coincide con el salto que cruza toda Australia (ver mapa), por lo que puede considerarse un error no tan terrible, dada la extensión del país.

En esta ruta tuvimos entonces dos *true positives* y dos *false negatives*.

Algo que puede valer la pena mencionar de este caso es que la mayoría de los valles donde el delta RTT da 0ms son saltos donde la diferencia de tiempo es menor que la varianza, lo cual es razonable ya que se mueven entre nodos que están cercanos entre sí.

IV. Discusión

Recapitulando, de lo dicho hasta aquí nos llevamos las siguientes conclusiones:

- Vimos, con el caso de Rusia, que este modelo es muy sensible a anomalías como los caminos asimétricos (que sospechamos que fue uno de los problemas), o las congestiones en la red (otra suposición). Este caso también ilustra una situación que no puede mejorarse con una valor de corte arbitrario (distinto de τ) dado que los verdades saltos continentales tienen un RTT diferencial menor a los falsos.
- Aún en el caso de Australia, donde no parecieron verse anomalías grandes, el modelo tuvo problemas, infiriendo falsos enlaces continentales. El modelo parece demasiado simple para lidiar con la arbitrariedad de qué es y qué no un continente. Es notable que, por cómo funciona el método de Cimbala (ver un outlier a la vez, y sacarlo), aunque se detecten en forma correcta los enlaces continentales primero, luego quedan un set de puntos intracontinentales donde una gran distancia puede resultar un outlier (que no lo era si considerábamos el set completo). Esto hace que un caso como el de Australia, pueda terminar reduciéndose a varios como el de Brasil, encontrando falsos positivos. Posibles soluciones a esto serían tener siempre en consideración el *big picture* de todos los puntos como parte del score. También podría devolverse la lista de outliers con un nivel de confianza sobre la posibilidad de que sean enlaces continentales o no. En definitiva, la influencia de la longitud de la ruta para el método actual es menor a lo que se esperaría.
- Entre un 10 y un 30 por ciento de los hops ignoraron la respuesta por time exceeded, esto nos llamó la atención ya que parece ser un número bastante alto, aunque investigando un poco descubrimos que este fenómeno no es para nada extraño. Las razones más comunes por lo que esto suele ocurrir parecen ser la configuración del hop para omitir la respuesta a estos mensajes y el bloqueo de paquetes desde el firewall según indica la documentación de traceroute [2] y el artículo provisto por la cátedra [3].

En definitiva, notamos que este modelo tiene muchas oportunidades de mejora, y no es lo suficientemente robusto como para poder ser usado seriamente como un de-

[2] http://web.mit.edu/freebsd/head/contrib/traceroute/traceroute.c
[3] https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_02.pdf

tector de enlaces intercontinentales. De hecho, salvo que se cuente con cierta metadata sobre el estado de la red, parece imposible tener un buen predictor, considerando la gran variedad de situaciones que se dan actualmente en las redes y que pueden meter ruido, desde congestiones hasta anomalías debidas a las topologías o los protocolos heterogéneos.