TP2: Rutas en Internet

GRUPO 9: Adrián Bonaccini, Natalia Enrique, Julián Len, Nicolás Len

Departamento de Computación
FCEyN - UBA

10.11.2017

Resumen

El siguiente trabajo práctico tiene como objetivo analizar la ruta que se establece entre dos hosts a través de envíos de paquetes ICMP. Se intentará reconstruir la topología de la misma utilizando como herramienta un traceroute propio y algunas nociones de probabilidad para reconocer los enlaces tanto continentales como intercontinentales.

I. Introducción

El objetivo del presente trabajo es poder analizar las rutas que toman los paquetes cuando son enviados a través de Internet. Se propondrá para tal fin estudiar los recorridos parciales de cada uno de ellos haciendo uso del parámetro **Time To Live** (TTL de ahora en adelante). El mismo es un campo que se encuentra dentro del paquete IP, que cada router que lo recibe se encargará de decrementarlo para evitar la circulación indefinida por la red.

En base a esto se implementará un algoritmo de traceroute para obtener los tiempos de **Round Trip Time** (RTT de aca en adelante) y finalmente se aplicará el método de obtención de outliers de **Cimbala** para detectar posibles saltos intercontinentales.

Dado que las redes de gran escala, como Internet, generalmente son operadas por entidades administrativas diferentes, la información completa y actualizada sobre la topología y el estado de la red suele ser difícil de obtener. En muchos casos, las mediciones tomadas con traceroute son la única forma de obtener dicha información. Las conclusiones extraídas de la salida de la herramienta suelen ser la única forma de diagnosticar el flujo de las rutas. Sin embargo, el traceroute clásico no se construyó con una tecnología de gestión de redes moderna en mente, por lo que a menudo genera resultados falsos o anómalos. Por esto mismo, es nuestra intención usar distintos criterios para mitigar la mayor cantidad de estas anomalías y lograr una idea acabada del estado de la red. [1]

II. Desarrollo de la Herramienta y Métodos

Para la implementación de esta herramienta nos basamos en el intercambio de mensajes de tipo `echo request/reply` y `time exceeded` del protocolo `ICMP`. Para ello utilizamos la biblioteca `Scapy` para `Python` que permite el modelado y envío de paquetes. Construyendo y armando paquetes `ICMP` con TTLs de forma incremental, se los envía individualmente y en ráfagas al host destino, chequeando para cada uno de ellos si la respuesta es del tipo `time exceeded` y, en ese caso, se lo trata como un nodo intermedio entre el host origen y el destino. Luego lo agregamos a la ruta estimada del paquete. En caso de obtener como respuesta `echo reply` quiere decir que llegamos al destino. Para poder hallar la ruta más probable y estimar mejor los tiempos de respuesta del paquete, enviamos ráfagas de tamaño 50 (esto es, para asegurarnos de respetar el mínimo de 30 respuesta de tipo time exceeded) por cada TTL y por cada una de ellos guardamos el host que respondió junto con el RTT. Cabe mencionar que podemos encontrarnos con mensajes que no contengan una respuesta válida para la construcción de la ruta. Esto puede deberse a que los routers (incluso firewalls) se encuentren configurados para no responder a este tipo de mensajes ICMP. En este caso la decisión que tomamos fue proceder a descartar el salto ante un máximo de 5 respuestas con timeouts seguidas. Asumimos que el resto de la ráfaga tendrá el mismo comportamiento y el resto de los valores del hop los guardamos con valores

nulleados. Esta es una de las simplificaciones del modelado de la ruta que estamos aplicando. El camino entre dos nodo de nuestro modelo puede contener algún otro en el medio al que no podemos acceder. Dicha anomalía(**missing hops**) se encuentra detallada en el paper de referencia [1]

Finalmente con los promedios obtenidos para cada salto válido (omitimos timeouts e IPs privadas) calculamos los RTTs entre ellos de la siguiente forma:

$$\text{RTT}_i = \text{RTT}_i \text{ - } \text{RTT}_{i-1}$$

Existe otro escenario en donde se pueden encontrar inconsistencias en las mediciones: cuando el RTT del host anterior (i-1) es mayor al actual(i). Esta situación podría deberse a muchos factores, entre ellos al trafico esporádico (congestión) entre los enlaces. Es decir, cuando el algoritmo explora un nuevo salto (incremento del TTL), podría existir mayor congestión para llegar allí que cuando lo hizo para el salto anterior. Es decir, el tiempo de encolamiento en cada router es altamente variable. Más aún, podría ocurrir que ciertos nodos le den una baja prioridad a las respuestas ICMP. Si bien el envío en ráfagas intenta aproximar los tiempos para cada salto, entre saltos la realidad puede ser muy distinta.

Es así que, durante la etapa experimental, encontramos frecuentemente este escenario que, de alguna manera, empobrecía el método de detección de los saltos intercontinentales. Como el método de detección de outliers de **Cimbala** [2] se basa en las muestras de una distribución, podemos solo proveerle con aquellas mediciones que tengan una relación coherente (incremental) en el tiempo entre los saltos. Se filtran aquellos nodos que no cumplen con ello y luego de aplicar el test para los restantes, revisamos manualmente si son representativos de un salto intercontinental o no. Además para evitar posibles falsos positivos vamos a eliminar también aquellos saltos en los cuales la IP es privada. En resumen, una vez finalizada la obtención de la ruta del paquete, nos enfocamos en determinar si los saltos son intercontinentales. Para ello, nos basamos en método de obtención de Outliers de **Cimbala**. En cuanto al test, se puede ampliar su lectura en el paper de referencia de **Cimbala**. Básicamente se computan las diferencias entre el promedio de la muestra y cada muestra para luego dividirlo por el desvío estándar. Se ordenan estos valores y se toma el más grande. Si dicho valor supera un **cut-off** que depende del tamaño de la muestra, se elimina de la misma y se repite el proceso. Si no lo supera, entonces no es un outlier. Más aún, no hay otro outlier en la muestra.

Notar que un outlier en la muestra, según nuestras hipótesis, se corresponde con un salto intercontinental. También pueden ocurrir comportamientos anómalos, como excesivo tráfico en los routers y el correspondiente incremento en los tiempos de respuesta, que luego se traduzcan en falsos positivos. En un escenario ideal cuando no ocurren ninguna de las anomalías mencionadas, los RTTs entre saltos aumentan a medida que se incrementa el TTL.

III. Muestras

Con el fin de tener muestras distribuídas en el planisferio, escogimos distintas ciudades alrededor del mundo. Nótese que las ciudades están alejadas entre si, nuestra intención es encontrar distintas rutas de manera de que el camino hacia el host destino tenga distintos nodos intermedios y pase por distintos enlaces.

Cabe mencionar que dado que estamos intentando destacar saltos intercontinentales, se eligieron ciudades que cumplan ese requisito para asegurarnos que encontraremos al menos un salto intercontinental en cada destino.

Las destinos elegidos corresponden a los siguientes países:

- Australia
- Islandia
- Japón
- India

IV. Resultados de Experimentación

1. Australia

Para la siguiente muestra, utilizamos como host la web *sydney.edu.au* de **The University of Sydney**. Para asegurarnos que la muestra de información es confiable, calculamos para todos los saltos, cuantos respondieron con IPs privadas y/o RTT negativos, ya que

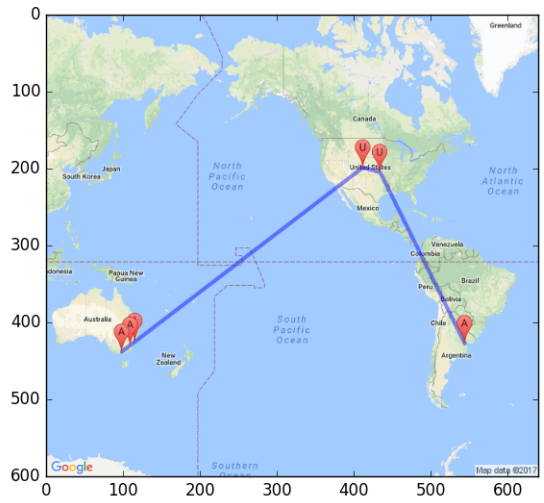
estos saltos decidimos descartarlos. Lo mismo con aquellos saltos intermedios que respondieron con IPs privadas. El resultado fue el siguiente:

Cuadro 1

Australia	
Timeouts	8
RTT negativos	8
IPs privadas	1
Saltos totales	30

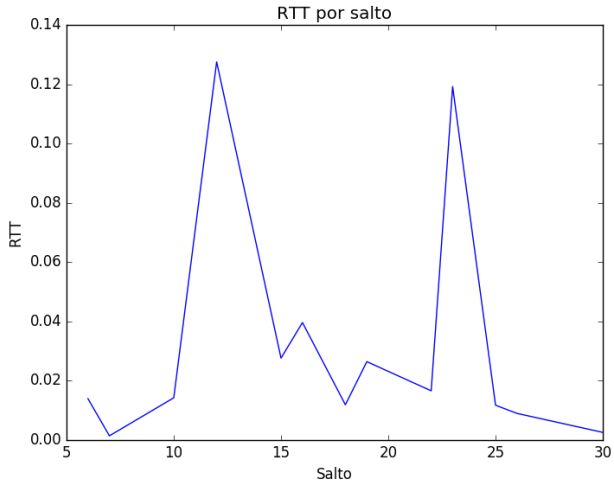
Como podemos observar de 30 saltos, 8 dieron Timeouts, además se encuentra el salto que responde *echo reply* esto nos da un porcentaje de **30** % de saltos que no respondieron Time Exceeded (contando aquellos con IP privada y RTT negativa). Luego si contamos el largo como los saltos que responden positivamente Time exceed, el mismo sería de 21 saltos.

Luego al procesar los resultados y ver los saltos intercontinentales, podemos observar la ruta real de los paquetes. Para esto, se tomaron las IPs de aquellos paquetes cuyo RTT no fue negativo ni su IP correspondía con una privada, y las localizamos en el mapa. El resultado fue:



Como se puede ver, existen 2 saltos intercontinentales: de Argentina a Estados Unidos y de allí hacia Australia.

Para poder comparar si la distribución de RTT entre saltos (sin tomar en cuenta las IPs privadas ni aquel cuyo RTT es negativo) presenta outliers según el método Cimbala, imprimimos en un mapa el resultado de suponer los outliers como saltos intercontinentales. Podemos hacer un primer acercamiento a la decisión de Cimbala observando el siguiente gráfico:

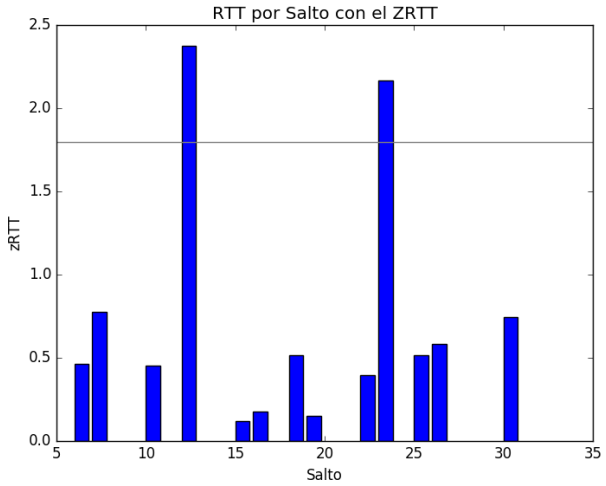


Donde el gráfico muestra que ciertos RTTs se destacan del resto nos permite inferir que se tratan de los saltos intercontinentales.

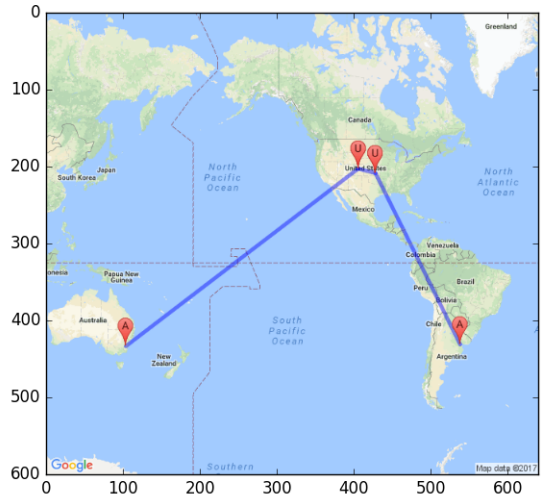
Además complementamos los resultados con el siguiente gráfico que muestra, dado el τ_n (constante que se obtiene a través de Cimbala)y sea x_i el RTT del i-ésimo salto, $\overline{X}$ el promedio de los RTTs de cada salto y **S** el desvio standard, se calculó:

$$\frac{|\overline{X} - x_i|}{S}$$

Luego se graficó por cada RTT el resultado de hacer la cuenta anterior y el resultado que se obtuvo fue:



En estos gráficos corroboramos que existen dos posibles saltos intercontinentales (dado los picos del primer gráfico y los dos del segundo). Luego utlizamos los resultados que se obtuvieron de encontrar outliers con Cimbala y ubicamos los mismos en un mapa obteniendo el siguiente:



Finalmente Cimbala encontró dos outliers que corresponden con los saltos intercontinentales presentes en el mapa. Además, coinciden con los saltos intercontinentales analizados con los datos reales. Dado que no se encuentra ningún salto intercontinental nuevo ni se eliminó ninguno con respecto al mapa con los datos reales (obtenidos con la biblioteca GeoIP), se puede concluír que no hubo falsos positivos ni negativos.

II. Islandia

Para el siguiente experimento las muestras fueron tomadas al host de la web *english.hi.is*, perteneciente a **University of Iceland**.

Aplicando nuestra herramienta, se obtuvieron los siguientes resultados:

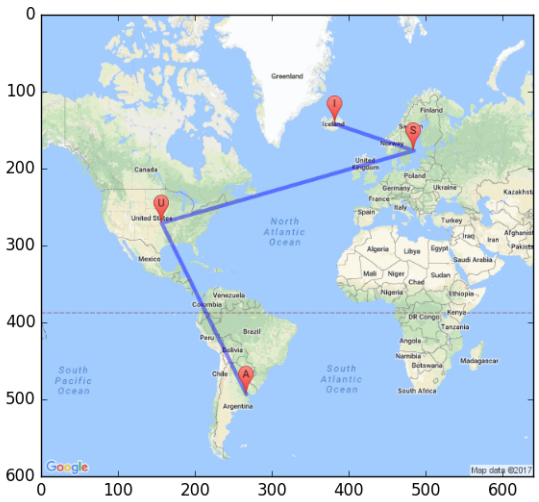
Cuadro 2

Iceland	
Timeouts	7
RTT negativos	7
IPs privadas	1
Saltos totales	26

Podemos notar que, de un total de 26 saltos, obtuvimos 7 categorizados como timeout. Quitando aquel salto de tipo *echo reply* tenemos un **28** % de saltos que no responden *time exceeded* sobre la muestra.

Obteniendo así un largo total de la ruta de 19 saltos (incluyendo IPs privadas y RTTs negativos).

Antes de ver los resultados que arrojó el método Cimbala queremos ver a través de las respuestas obtenidas, cuál es la ruta real que tomaron los paquetes. Para ello, tomamos las IPs de aquellos paquetes tales que no obtuvieron RTT negativo y no correspondían a IPs privadas y las localizamos en un mapa. Así obtuvimos:

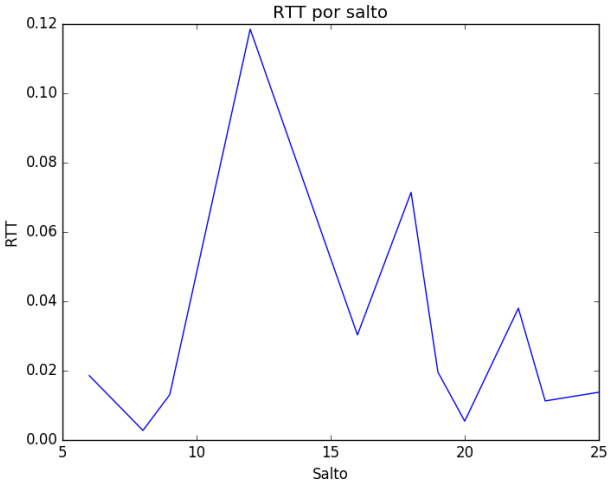


Tomando la noción de Europa Continental [3] Se puede notar que la ruta tiene 3 saltos intercontinentales que corresponden de Argentina - Estados Unidos,

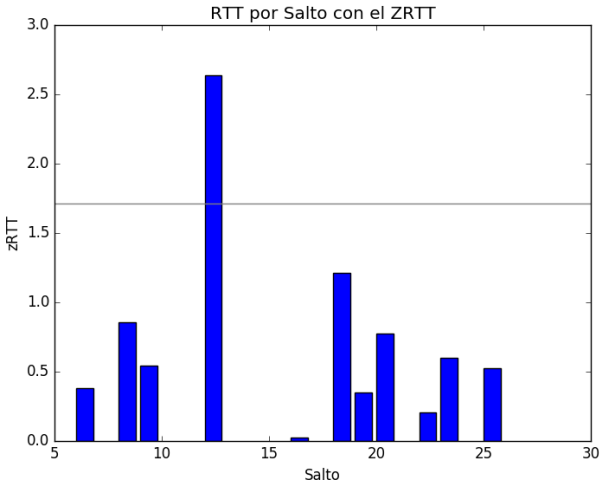
Estados Unidos - Suecia y Suecia - Islandia.

Ahora, queremos corroborar si utilizando el método de Cimbala obtenemos los mismos resultados.
Al igual que para el mapa original, vamos a filtrar aquellas IPs privadas, aquellos paquetes que respondieron time out y aquellos para los que obtuvimos un RTT negativo entre saltos.

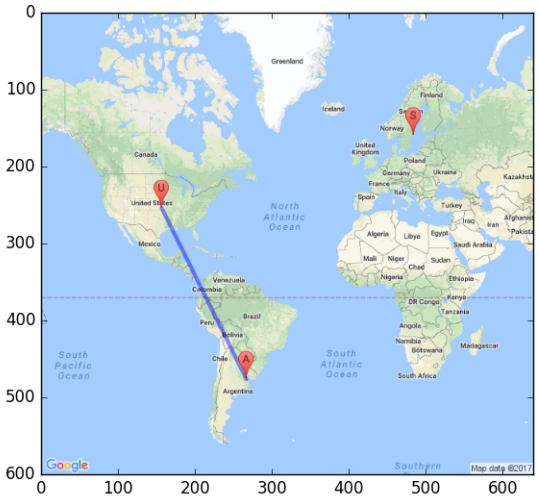
Antes de ahondar sobre la detección de saltos a través del método, veamos si en el gráfico de RTT por saltos podemos notar una diferencia interesante de tiempos que podrían marcarnos outliers en nuestra muestra.



En principio, tenemos tres picos que podrían sugerir los tres saltos que estamos buscando.
Una vez realizados los cálculos que Cimbala precisa, vamos a estudiar los resultados obtenidos en el siguiente gráfico que representa el ZRTT entre saltos.



Tal como menciona el material de referencia, podemos detectar outliers, si para una muestra dada el valor Z es mayor al tau.
Cabe destacar que el valor tau que se grafica, pertenece al último elemento que fué tomado como mayor.
Recordemos que para calcular los outliers, una vez que detectamos uno, lo quitamos de la muestra original y volvemos a realizar las cuentas con la esperanza de hallar otros.
Si bien en nuestro gráfico de RTTs por salto pareciera que tenemos tres saltos, en éste gráfico sólo podemos detectar uno.
Finalmente, con el resultado que Cimbala nos arrojó, obtuvimos el siguiente mapa:



Podemos ver en el mapa que se obtuvieron 2 saltos

intercontinenales y no uno como nos arrojó el gráfico anterior, por lo que podemos decir que, para este caso, el gráfico representado no nos arrojó un resultado preciso como así lo hizo en el caso de Autralia.
Además, sólo obtuvimos un salto que se corresponde con el mapa original, aquel que va de Argentina a Estados Unidos.
El punto aislado, se corresponde a un salto que fue hecho dentro del mismo territorio, es decir, que la IP source y destino pertenecían al mismo país.
En ocasiones como éstas, en las que el método nos arroja como salto intercontinental un salto que no lo es, los distinguiremos como falsos positivos.
Además, viendo nuestros resultados versus el mapa original, podemos asegurar que tuvimos dos falsos negativos, que se corresponden a los dos saltos faltantes.
Por lo que podemos concluir que para esta ruta el método de detección de outliers de Cimbala no fue efectivo siendo los valores de la distribución muy similares como para que se destacara mas de uno.

III. Japón

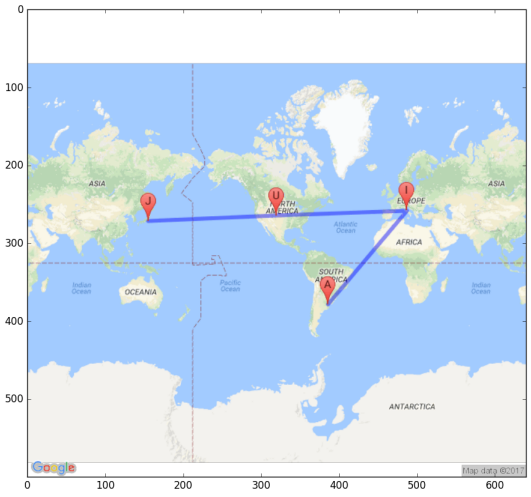
Para el siguiente experimento las muestras fueron tomadas al host de la web *www.u-tokyo.ac.jp*, perteneciente a **The University of Tokyo**. Aplicando nuestra herramienta, se obtuvieron los siguientes resultados:

Cuadro 3

Japon	
Timeouts	7
RTT negativos	9
IPs privadas	1
Saltos totales	28

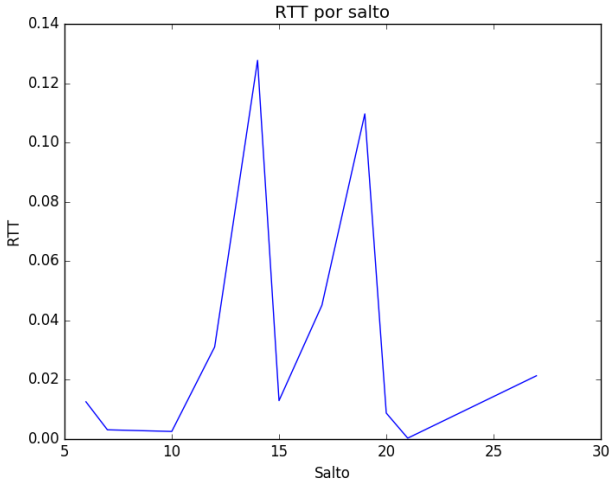
Veamos que de un total de 28 saltos obtuvimos 7 los categorizamos como timeout. Quitando aquel salto de tipo *echo reply* tenemos un **25,92** % de saltos que no responden Time exceeded sobre la muestra.
Obteniendo así un largo total de la ruta de 21 saltos (incluyendo IPs privadas y RTTs negativos).

Una vez que obtuvimos la ruta hacia destino, vamos a eliminar aquellos paquetes que corresponden a IPs privadas, aquellos en los que no obtuvimos respuesta (timeouts) y por último los que nos dieron un RTT negativo entre saltos. Una vez realizado ese filtro, tomamos las IPs y trazamos un mapa con la ruta del paquete.



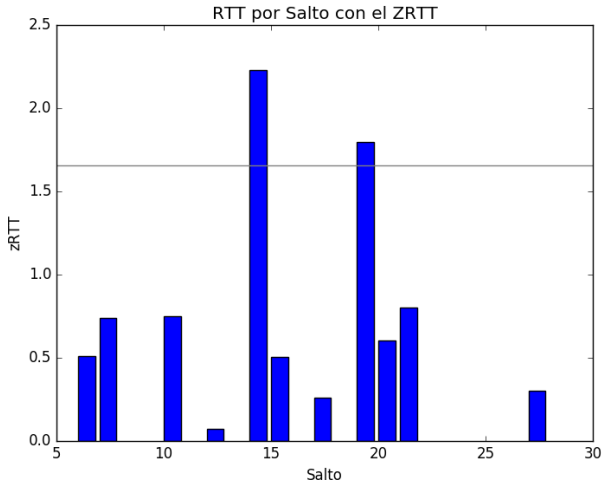
Podemos ver fácilmente que para esta ruta tenemos tres saltos intercontinetales pertenecientes a: América del Sur - Europa, Europa - América del Norte, América del Norte - Asia.

Nos gustaría, una vez aplicado el método de Cimbala para detección de outliers, poder conseguir la misma traza según los tiempos calculados en nuestro traceroute quitando aquellos que fueron mencionados con anterioridad.
Comencemos observando el RTT entre saltos del paquete para ver si a simple vista es posible detectar si tenemos, al menos, la misma cantidad de saltos.

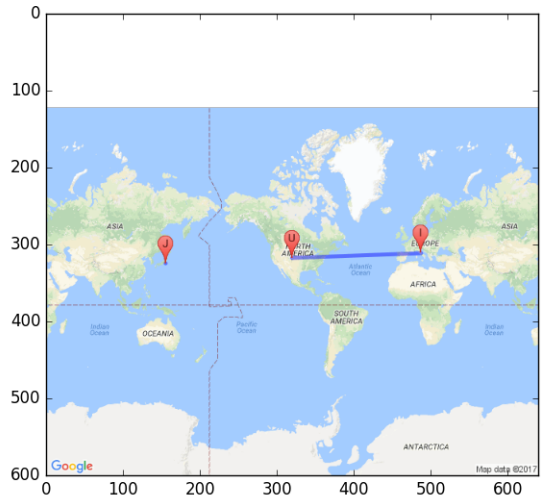


En este gráfico podemos notar 2 picos importantes por lo que, en principio, nos faltaría solo un salto. Esto nos da un acercamiento de que nuestros resultados podrían no ser los esperados.

Ahora, para estos mismos resultados, vamos a aplicar el método de Cimbala y graficar el valor Z de cada RTT entre saltos. Tomaremos como valor de corte, el tau perteneciente a la última iteración del método.



Tal como lo indica el corte, tenemos dos outliers candidatos a saltos intercontinentales.
Para verificar su procedencia tomaremos las IPs destino y source de ellos y los ubicaremos en un mapa.
Si bien hasta el momento obtuvimos dos outliers, y nuestro mapa original tiene tres, queremos ver que, al menos, los resultados obtenidos se correspondan con alguno de ellos.



Finalmente, en este último mapa podemos ver que de los dos outliers detectados, sólo uno se corresponde con alguno de los tres reales. Podemos concluir entonces que, con el método de Cimbala, obtuvimos un resultado correcto (Europa - Asia), un falso positivo (correspondiente al punto en el mismo lugar) y dos falsos negativos (América del Sur - Europa y América del Norte - Asia) por lo que podemos decir que para esta ruta, el método de detección de outliers de Cimbala no fue eficiente.

IV. India

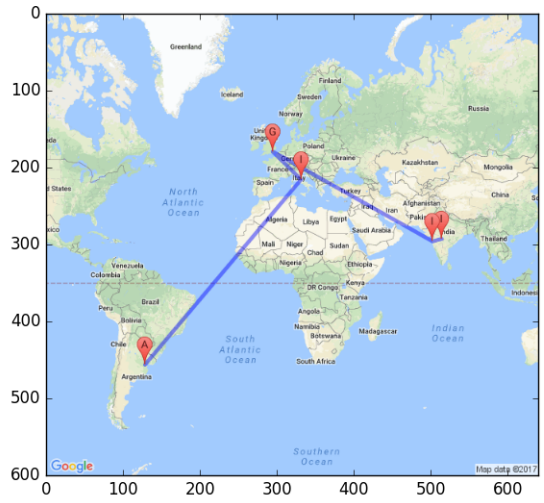
En esta muestra, utilizamos como host la web *mhrd.gov.in* de **Department of School Education And Literacy** . Al igual que las anteriores muestras, por cada salto calculamos y descartamos aquellos que dieron timeout. Además para asegurarnos que la muestra de información confiable calculamos, para todos los saltos, cuántos fueron con IPs privadas y/o RTT negativos, ya que estos saltos serán descartados. El resultado fue el siguiente:

Cuadro 4

India	
Timeouts	8
RTT negativos	2
IPs privadas	1
Saltos totales	18

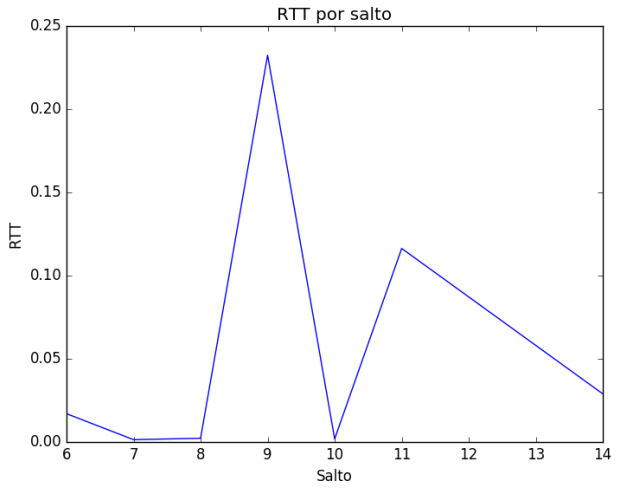
En este caso hubieron 18 saltos, 8 dieron timeouts, además se encuentra el salto que responde *echo reply* esto nos da un **44.4** % de saltos que no respondieron Time Exceeded (contando aquellos con IP privada y RTT negativa). Luego el largo de la ruta en término de saltos intermedios que responden positivamente al envío del paquete ICMP es de 10 saltos.

Al analizar las IPs (no privadas) de los paquetes cuyo RTT sea positivo, pudimos localizarlas en el mapa y ver su recorrido:



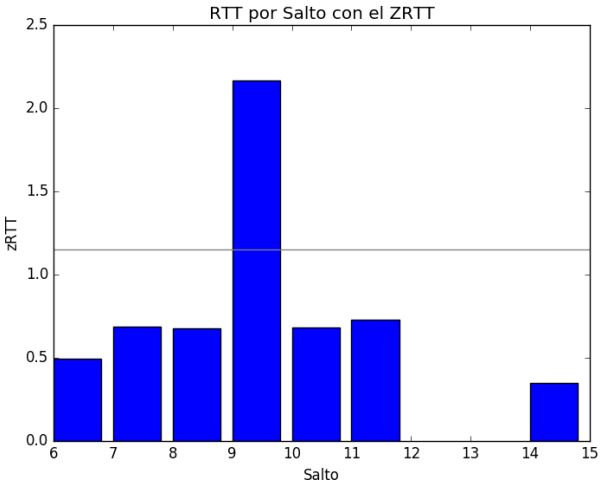
Como se puede observar, existen dos saltos intercontinentales, desde America del Sur a Europa, y desde Europa hacia Asia. Pero como fue mencionado en la muestra de Islandia, seguimos el criterio de **Europa Continental[3]**, entonces diremos que la cantidad de saltos intercontinentales fueron 3, de Argentina a Italia, de Italia a Reino Unido, y de este último a India.

Para poder comparar si la distribución de RTT entre saltos (sin tomar en cuenta las IPs privadas ni aquel cuyo RTT es negativo) presenta outliers según el método Cimbala, en principio observamos los distintos RTT entre saltos:

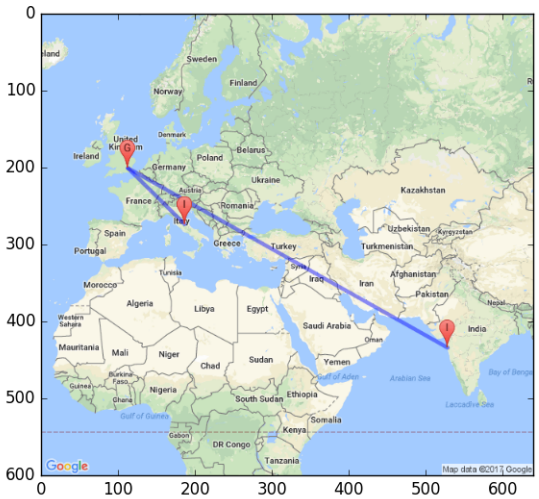


En principio, únicamente encontramos dos picos en el gráfico, lo que nos da un indicio de que Cimbala habrá arrojado como resultado que únicamente existieron dos saltos intercontinentales.

En sintonía con los resultados obtenidos para **Islandia**, los siguientes resultados fueron obtenidos al graficar RRTs por salto respecto del ZRTT:



Al igual que el anterior gráfico, aparentemente existirán únicamente dos saltos intercontinentales. Procedemos a ubicarlos en el mapa aquellos saltos intercontinentales que arrojó el método de Cimbala:



Exactamente como se había pensado, Cimbala arrojó que únicamente existen dos saltos intercontinentales (tomando en cuenta, nuevamente el criterio de Europa Continental), estos son de Italia a Reino Unido, y de este último a India.

Podemos observar que entre el mapa arrojado por

el recorrido real, y el de Cimbala, existen ciertas diferencias. Es decir, Cimbala no tomó en cuenta el salto Argentina-Italia como intercontinental. Esto es equivalente a que Cimbala arrojó un falso negativo. Mientras que el resto de saltos resultantes por Cimbala, sí coinciden con los enlaces intercontinentales esperados por el análisis.

V. Resultados globales y conclusiones

A lo largo del trabajo descubrimos que las rutas que toman los paquetes IP en Internet (al menos los del tipo ICMP) siguen rutas que son altamente cambiantes. Es dificil medir los verdaderos RTT por las diferentes variables que pueden alterar el comportamiento: desde la carga por tráfico en las rutas, firewalls involucrados, routers que usan MPLS, etc. Por esta razón, inferir la topología detrás de alguna parcialidad de Internet es una tarea ardua a partir de la herramienta que se propone y genera en principio lo que se denomina como *anomalías*. Las anomalías que se encontraron en nuestras muestras fueron:

- **Missing Hop**: Esta anomalía ocurre cuando un router tiene configurado no generar respuestas del tipo ICMP TTL Exceeded. Lo cual en todas las muestras se traduce en saltos clasificados como timeouts en los cuales nulleamos toda la información para cada campo.
- **False RTT**: Esta anomalía refiere a tiempos falsos reportados por el traceroute. Esto impide reflejar a través de la comparación entre los tiempos de los saltos el tiempo que le lleva a un paquete llegar al host destino. En nuestras muestras se dieron estos casos de RTT negativos". Ante esta anomalía nosotros decidimos que, si la cantidad de RTT negativos para una muestra era considerable, cambiaríamos el host destino por uno menos limitado. En el caso en que no fueran representativos en la cantidad, los descartaríamos. Las causas a las que este comportamiento se debe son varias, entre ellas, la implementación de MPLS de algunos routers, balance de carga, asignación de prioridades a las respuestas de mensajes ICMP, tiempos de encolado, entre otros. Si tomamos nuestra muestra, de un total de 47 saltos 26 dieron RTT negativos, esto es un 55 %.

Además de esto, no observamos ningún otro comportamiento anómalo.

Tomando ciertas precauciones, como desestimar los nodos que evidenciaron este comportamiento descripto, nos fue posible hacer un análisis más certero. Cabe mencionar en este punto que, para algunas rutas, se hizo uso del concepto de Europa continental. Tanto en el caso del experimento a Islandia (salto de Suecia a Islandia) como en el caso del experimento a India (salto de Reino Unido a Italia), decidimos ser consistentes con el criterio y clasificamos este tipo de saltos también como intercontinentales.

Otra salvedad que queremos hacer es que, al momento de la detección de los saltos intercontinentales, aquellos destinos que tenían más de tres saltos en la ruta, siempre encontramos falsos positivos y/o negativos. Nunca nos fue posible hallar la totalidad de ellos a través del método de detección de outliers provisto por Cimbala.

Tomando en cuenta los resultados que dicho método arrojó, obtuvimos ocho candidatos a saltos intercontinentales de un total de once efectivos que notamos contrastando con el mapa que generamos con la biblioteca GeoIP. Entre los candidatos hubo un porcentaje de 62,5 % falsos negativos y 25 % falsos positivos. Es decir que de los ocho candidatos que obtuvimos en los distintos experimentos, más de la mitad arrojó falsos negativos, es decir que los saltos intercontinentales reales no fueron tomados en cuenta por el método, lo cual nos parece más grave pues no estaríamos teniendo un buen porcentaje de confiabilidad en el método.

Finalmente, se lograron identificar seis de once saltos intercontinentales, es decir el 54 % de ellos, si bien este porcentaje es relativamente bueno, no obtenemos confiabilidad en el método, pues por el análisis realizado anteriormente obtenemos un porcentaje de falsos negativos lo suficientemente alto como para desconfiar del mismo.

Queda pendiente poder intentar descubrir algún valor que sirva como un cut-off que distinga los saltos intercontinentales con mayor eficiencia.

VI. Referencias

- [1]: Traceroute Anomalies - Martin Erich Jobs (http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_02.pdf)
- [2]: Cimbala (http://www.mne.psu.edu/cimbala/me345/Lectures/Outliers.pdf)
- [3]: Europa Continental (https://en.m.wikipedia.org/wiki/Continental_Europe)