Trabajo Práctico 2: Traceroute

15 de noviembre de 2016 — Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Arribas, Joaquín Manuel	702/13	joacoarribas@gmail.com
Forte, Martín	363/10	martinlforte@gmail.com
Lebrero Rial, Ignacio Manuel	751/13	ignaciolebrero@gmail.com
Vázquez, Jésica	318/13	jeesivazquez@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

1. Introducción

En este trabajo práctico desarrollamos una herramienta de *traceroute* en Python utilizando las librerías scapy para el envío de paquetes a distintas universidades del mundo. Además utilizamos las herramientas *numpy* y *scipy* para realizar estadísticas, como el cálculo de la media, la desviación estándar, y el uso de la tabla *t de Student*, entre otras.

2. Metodología

Nuestra implementación de *traceroute* se divide en dos etapas: múltiples trazados de ruta, y luego estimación de cuál de esas rutas es el camino más probable al destino. Para la primera etapa, utilizamos la técnica de enviar paquetes con un TTL que se vaya incrementando de forma de ir recibiendo las direcciones IP de donde recibimos respuesta. Luego, la herramienta permite calcular la ruta más frecuente por donde se envíaron los mensajes ICMP *Echo Request* y se obtuvo una respuesta. Cabe destacar que muchos webservers tienen deshabilitada la respuesta de los mensajes ICMP o bien filtrados, por esta razón, en caso de que obtengamos un timeout por falta de respuesta, reintentamos con un sync al puerto 80 con el mismo ttl para así, de obtener una respuesta, poder tomar como que se llegó al destino.

A continuación se utilizará esta herramienta para hacer *traceroute* a distintas universidades en el mundo y analizar el comportamiento de la detección de *outliers* a partir del método de *Cimbala*. Al analizar los resultados provistos por este método podremos corroborar la información obtenida con la información exacta que podemos obtener de los *hosts* visitados, planteando posibles hipótesis sobre los *outliers* detectados por el método.

Cabe destacar que a la hora de encontrarnos con datos ruidosos, donde *hosts* más lejanos en el camino tenían un menor *rtt* que los encontrados antes, tomamos una decisión particular sobre cómo calcular el *rtt* entre dicho *host* y su inmediato anterior:

- Si un *host* tiene menor *rtt* que alguno encontrado previamente (es decir, llegar hasta ahí desde el anteúltimo nodo recorrido del camino consume un *rtt* negativo), consideramos que el *rtt* consumido para llegar allí es cero.
- Si un *host* tiene el mayor *rtt* hasta el momento, pero los nodos previos por los cuales paso el camino tenían un *rtt* negativo, el tiempo consumido para llegar allí será la diferencia entre el *rtt* del *host* actual menos el *rtt* del último nodo que no tuvo *rtt* negativo.

Para ejemplificar:

TTL	RTT total del camino	RTT entre el nodo actual y sus anteriores
2	2.3	2.3
3	1.9	0
4	2.1	0
5	2.7	0.4

Cuadro 1: Ejemplo de cálculo de *rtts* entre dos *hosts* en el camino

Los *hosts* correspondientes a los *TTLs* 3 y 4 tienen una diferencia de *rtt* con sus anteriores igual a cero ya que tienen menor *rtt* que *host* correspondiente al *TTL* 2.

La diferencia de *rtt* del último *host* se calcula teniendo en cuenta al último valor no negativo, correspondiente al *TTL* 2.

3. Requerimientos y modo de uso

3.1. Requerimientos

Para correr el TP son necesarios:

- Python 2.X
- Scapy
- GeoIP: Para instalarlo: pip install python-geoip-geolite2
- numpy
- scipy

3.2. Modo de uso

python main.py –hostname hostname [–maxTtl maxTtl] [–traceAmount traceAmount] [–timeout timeout]

- -h, –help Muestra mensaje de ayuda.
- –hostname hostname Host al que se le quiere rutear.
- –maxTtl maxTtl Cantidad maxima de ttls que se van a intentar.
- –traceAmount traceAmount Cantidad de veces que se va realizar el trace para luego promediar.
- –timeout timeout Timeout por cada request. En segundos.

Ejemplo: *python main.py –hostname www.u-tokyo.ac.jp –traceAmount 5*

3.3. Herramientas utilizadas

Utilizamos las siguientes páginas de internet para verificar la veracidad de la localización de ips utilizadas por nosotros:

- `https://www.iplocation.net/`
- `https://geoiptool.com/`
- `http://www.plotip.com/`

4. Primer Experimento: Australia

4.1. Presentación

En el siguiente experimento se hizo un *traceroute* a la universidad de Sydney, Australia.
En particular, se utilizó la *URL* `sydney.edu.au` como dirección destino.

4.2. Motivación e Hipótesis

Teniendo en cuenta la distancia que existe entre América del Sur y Oceanía, y sabiendo además que la gran mayoría del tráfico, en general, se dirige hacia Estados Unidos y Europa, parece una buena idea preguntarnos qué caminos irán recorriendo los paquetes que enviamos. No creemos encontrar un camino directo entre Argentina y Oceanía.

Es también interesante preguntarse la efectividad del método elegido para detectar saltos intercontinentales, dado que por lo menos debería haber un salto importante para detectar. Aunque no estemos seguros del camino que realice, probablemente el salto que realice desde algún continente hacia Oceanía será detectado por el método de *Cimbala*, dado que es el continente más pequeño y está relativamente aislado del resto por océanos.

De todas maneras, no se puede descartar la posible aparición de otros enlaces intercontinentales, dependientes del camino elegido para llegar a destino.

4.3. Análisis de Resultados

A continuación presentaremos los resultados obtenidos luego de realizar el *traceroute*. Utilizaremos el algoritmo de detección de *outliers* para contrastar los datos recibidos con los datos que obtenemos de las IPs. De esta manera podremos concluir sobre la efectividad de dichos métodos.

Como el método de *outliers* depende del *rtt*, y es muy común encontrar variaciones importantes de *rtt* para nuestro *traceroute*, presentaremos el resultado que más seguido se recibió, que fue además relativamente efectivo. Este experimento fue realizado 100 veces y el camino encontrado fue casi siempre el mismo, exceptuando 5 iteraciones.

Obviaremos el *time exceeded* recibido del primer *ttl* debido a que es la respuesta que obtenemos del *router* correspondiente al lugar donde este experimento tuvo lugar[1], por lo cual no tiene mucha relevancia y no contribuye a mayor claridad en el experimento.

TTL	IP	RTT	Country	Continent	Cambió Cont. (Cimbala)	Cambió Cont. (Región IP)
2	191.85.0.1	0.26675	Argentina	América del Sur	No	No
3	*					
4	200.51.240.246	0.27806	Argentina	América del Sur	No	No
5	200.51.240.228	0.24336	Argentina	América del Sur	No	No
6	200.51.240.181	0.19772	Argentina	América del Sur	No	No
7	213.140.39.118	0.19782	España	Europa	No	Sí
8	5.53.5.154	0.32221	España	Europa	No	No
9	213.140.36.70	0.32144	España	Europa	No	No
10	213.140.52.229	0.31144	España	Europa	No	No
11	208.185.52.74	0.47221	Estados Unidos	América del Norte	Sí	Sí
12	202.158.194.176	0.62258	Australia	Oceanía	Sí	Sí
13	113.197.15.146	0.64370	Australia	Oceanía	No	No
14	138.44.5.47	0.60584	Australia	Oceanía	No	No
15	*					
16	*					
17	129.78.5.8	0.73426	Australia	Oceanía	No	No

Cuadro 2: ICMP Traceroute a 129.78.5.8

Obtuvimos 3 *hosts* que no respondieron nuestros mensajes (18 %) y 14 que sí pudieron ser reconocidos (82 %).

[1] Tienda del Cafe, Av. Santa Fe y Av. Callao

Este sería uno de los posibles caminos tomados por el *traceroute*. No descartamos que para llegar a Australia, en vez de cruzar el pacífico, el camino tomado haya sido por el atlántico. Las líneas rectas que comunican los distintos puntos son sólo a modo de ejemplo.

Figura 1: Posible camino realizado en el *traceroute*

4.4. Análisis general

Cabe destacar que obtuvimos 3 *TTLs* perdidos. El primer *TTL* perdido, se debe a alguna cuestión interna de *Telefónica Argentina*, ya que suceden en todos los *traceroutes* desde la máquina en que se realizó. También, los *TTLs* 15 y 16 se perdieron en todos los *traceroutes* realizados hacia el destino analizado. El *host* del nodo 14 corresponde a *AAARNet (Australian Academic and Research Network)*, encargada de proveer servicios de internet a los centros educativos y de investigación de Australia. Cómo la conexión con la universidad de Sydney se realiza a través de *AAARNet* hipotetizamos que los hosts de los *TTLs* 15 y 16 corresponden a una cuestión interna de ellos.

El paper *Traceroute Anomalies*[2] sugiere una explicación con mayor justificación. Podría ser que estos dos *routers* estén protegidos por un *firewall* que evita la respuesta a *echo requests*, o que por alguna otra razón, el administrador del *router* haya decidido deshabilitar las respuestas a mensajes del protocolo *ICMP*. Estas son algunas de las explicaciones posibles para reflexionar sobre las distintas anomalías que hemos encontrado en este experimento.

En particular, podemos evidenciar que para el algoritmo de *Cimbala* hubo:

- Un enlace intercontinental encontrado hacia **Norteamérica** desde Europa.
- Un Enlace intercontinental encontrado hacia **Oceanía** desde Norteamérica.

Por otro lado, analizando la región asignada a cada IP hubo:

- Un enlace intercontinental encontrado hacia **Europa** desde Sudamérica.
- Un enlace intercontinental encontrado hacia **Norteamérica** desde Europa.
- Un Enlace intercontinental encontrado hacia **Oceanía** Norteamérica.

Podemos comprobar aquí que el enlace que considerábamos el más importante fue el que nos llevaba hacia Oceanía, y este efectivamente fue detectado de manera exitosa. Para llegar a Oceanía el camino establecido pasó por Norteamérica, hecho detectado por el algoritmo de *Cimbala*. Por el otro lado el algoritmo de *Cimbala* no detecto el salto intercontinental hacia Europa.

Para comprender mejor por qué estos resultados fueron los obtenidos, vamos a representar los datos obtenidos de una forma más cercana a aquella en la que los analiza el algoritmo que creamos a partir de *Cimbala*.

Los siguientes gráficos muestran la diferencia relativa de *rtts*, además de los datos utilizados por el algoritmo de *Cimbala* para detectar *outliers*:

[2]Traceroute Anomalies, Martin Erich Jobst

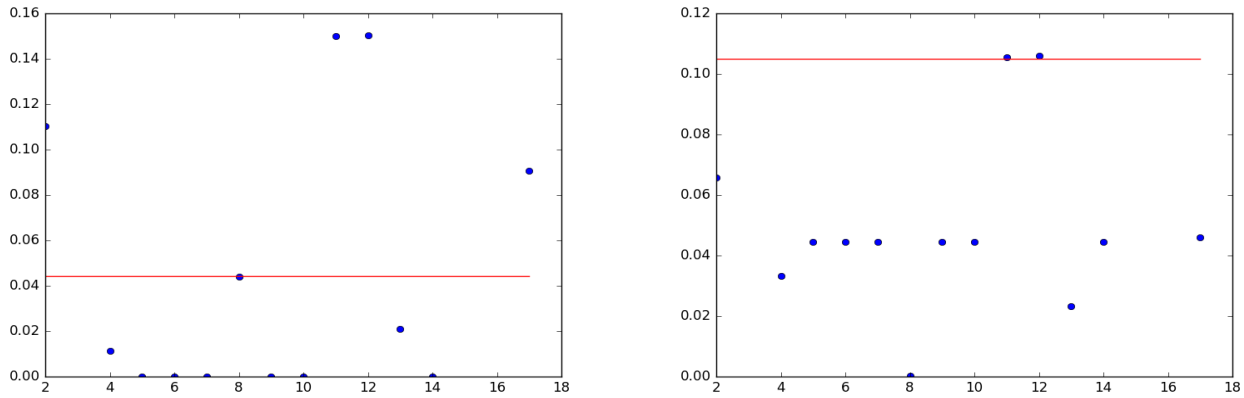

Figura 2: A la izquierda, la diferencia relativa de *rtts*. A la derecha, los datos utilizados por el método de *Cimbala* para detectar *outliers*

Como podemos ver, los saltos correspondientes a los saltos intercontinentales son detectados por *Cimbala* y significativamente distintos del resto.

Del gráfico de la derecha surge una observación interesante, el salto que es a Europa está lejos de ser considerado un *outlier*. Como para este experimento pusimos cero en donde los *rtts* daban negativo, el método de cimbala tuvo en más en cuenta como *outlier* esos valores, que uno relativamente chico como el salto intercontinental a España. Respecto de este mismo tema, es curioso que la diferencia significativa de *rtts* se puede evidenciar recién en el segundo *host* perteneciente a España, y no en el primero.

Respecto del gráfico de la izquierda, es interesante notar cómo varios valores no considerados *outliers* por el método de *Cimbala* quedán por arriba de la media. Respecto del salto a España (8) sólo podríamos pensar que tenemos una conexión directa con el proveedor de servicio de Europa (Telefonica International Wholesale Services, SL), por lo cual la diferencia de *rtts* es baja.

Es interesante preguntarse porque una vez que se ingresa a alguna de las empresas telefónicas (en nuestro caso la de Argentina y España) la diferencia de *rtts* empieza a ser negativa.

Podríamos decir que el algoritmo basado en el método de *Cimbala* funcionó para los datos provistos en este caso. De todas maneras es necesario que el sistema de detección sea acompañado por un análisis profundo respecto de los datos dado que son muy inestables los *rtts* de los *routers* y teniendo en cuenta sólo la información recibida, no se podrá hacer ser siempre un análisis confiable.

De todas maneras, nos parece interesante remarcar que aunque el método de *Cimbala* no reconoció la totalidad de los saltos intercontinentales, tampoco evidencio los mismos en casos donde efectivamente no lo eran.

5. Segundo Experimento: Sudáfrica

5.1. Presentación

En el siguiente experimento se realizó un *traceroute* a la Universidad de Cape Town, ubicada en Sudáfrica.

La *URL* utilizada fue *www.uct.ac.za*.

5.2. Motivación e Hipótesis

En este experimento se busca analizar si:

- El camino más probable pasara por Europa para luego ir hacia África.
- Si podría darse el caso en el que el camino atraviese el océano Pacífico, atravesando Asia para luego llegar a África.
- En cualquiera de los casos anteriores, ver si se realizan saltos previos por centro/norteamerica.

Como primer experimento, se buscó analizar el comportamiento de la ruta por defecto en diferentes horarios: mañana, tarde y noche. Esto es, para ver si la hora influye sobre el tráfico de los caminos a tomar. La motivación para este experimento es que podría llegar a darse que haya una *hora pico* de tráfico en la cual una zona determinada (ej: Europa del Oeste) este muy congestionada y se tome, en promedio, otra ruta para llegar a destino.

De todas maneras no obtuvimos resultados concluyentes al respecto: intentamos obteniendo datos en 3 horarios distintos (mañana, tarde y noche) pero ni los caminos ni los *rtts* fueron significativamente distintos. Por esta razón abandonamos el experimento.

5.3. Análisis de Resultados

TTL	IP	RTT	Country	Continent	Cambió Cont. (Cimbala)	Cambió Cont. (Región IP)
2	200.3.60.23	0.32518	Argentina	América del Sur	No	No
3	200.117.79.97	035446.	Argentina	América del Sur	No	No
4	190.225.252.162	0.32117	Argentina	América del Sur	No	No
5	195.22.220.37	0.43685	Italia	Europa	No	Sí
6	89.221.41.181	0.59346	Estados Unidos	América del Norte	Sí	No
7	89.221.41.181	0.37317	Estados Unidos	América del Norte	No	No
8	154.54.9.17	0.43955	Estados Unidos	América del Norte	No	No
9	154.54.80.41	0.3456	Estados Unidos	América del Norte	No	No
10	154.54.24.193	0.36381	Estados Unidos	América del Norte	No	No
11	154.54.7.157	0.49044	Estados Unidos	América del Norte	No	No
12	154.54.40.105	0.37468	Estados Unidos	América del Norte	No	No
13	154.54.30.186	0.4865	Estados Unidos	América del Norte	No	No
14	154.54.57.154	0.62719	Estados Unidos	América del Norte	No	No
15	154.54.56.238	0.59983	Estados Unidos	América del Norte	No	No
16	149.14.80.210	0.52128	Estados Unidos	América del Norte	No	Sí
17	196.32.209.170	0.791533	Sudáfrica	Africa	Sí	No
18	155.232.6.65	0.58714	Sudáfrica	Africa	No	No
19	155.232.6.205	0.70377	Sudáfrica	Africa	No	No
20	155.232.32.14	0.70424	Sudáfrica	Africa	No	No
21	137.158.158.44	1.00372	Sudáfrica	Africa	No	No

Cuadro 3: ICMP Traceroute 181.91.163.40

Interesante destacar que en este experimento todos los *hosts* respondieron a los mensajes.

Tomando las ips resultantes, este sería un posible camino.

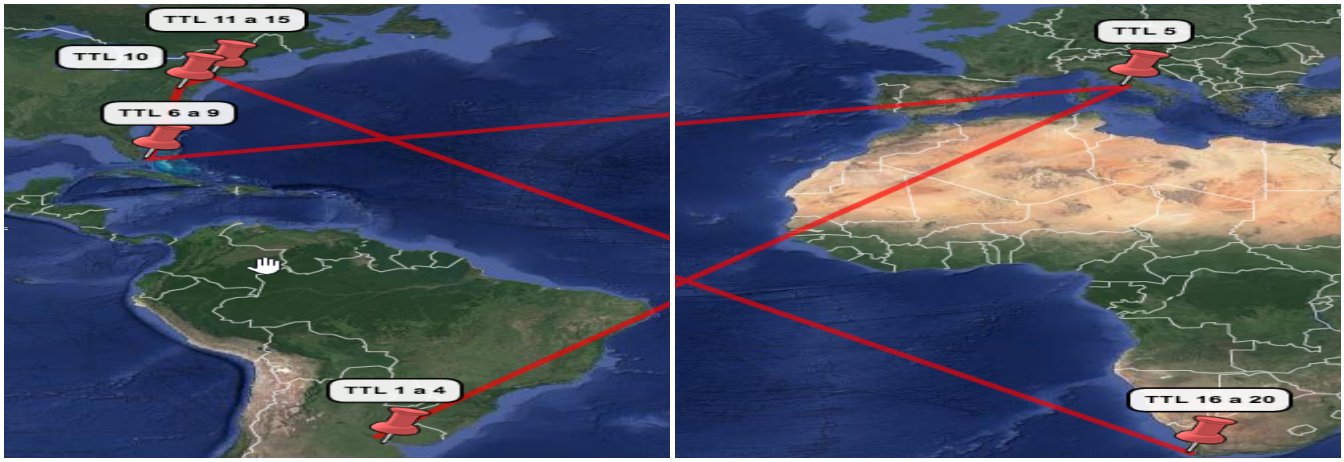

Figura 3: Posible camino realizado en el *traceroute*

5.4. Análisis general

En particular, podemos evidenciar que para el algoritmo de *Cimbala* hubo:

- Un enlace intercontinental encontrado hacia **Norteamérica** desde Europa.
- Un enlace intercontinental encontrado hacia **África** desde América del Norte.

Por otro lado, analizando la región asignada a cada IP hubo:

- Un enlace intercontinental encontrado hacia **Europa** desde América del Sur.
- Un enlace intercontinental encontrado hacia **Norteamérica** desde Europa.
- Un Enlace intercontinental encontrado hacia **África** desde América del Norte.

A continuación analizaremos para cada *TTL* el *host* y la localización, hipótetizando respecto de si el camino es el supuesto o no:

- El *host* correspondiente a los *TTLs* 2 y 3 fue Telecom BBIP
- El *host* correspondiente a los *TTLs* 4 a 5

Los siguientes gráficos muestran la diferencia relativa de *rtts*, además de los datos utilizados por el algoritmo de *Cimbala* para detectar *outliers*:

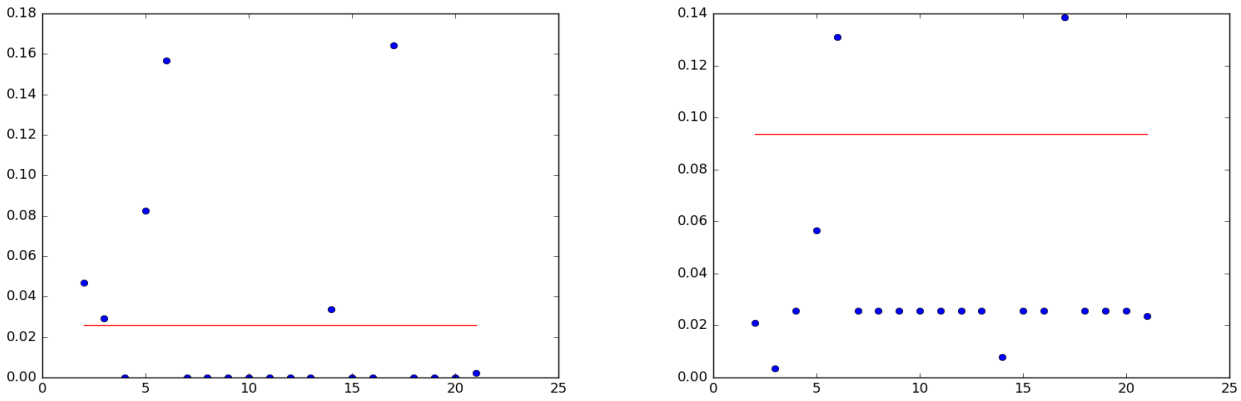

Figura 4: A la izquierda, la diferencia relativa de *rtts*. A la derecha, los datos utilizados por el método de *Cimbala* para detectar *outliers*

Podemops observar que el método de *Cimbala* evidencio 2 de 3 saltos intercontinentales. Por el otro lado uno de ellos (Italia) no demostró evidencia significativa como para ser detectado por un método de detección de *outliers* dada la muestra en l

6. Tercer Experimento: Rusia

6.1. Presentación

En el siguiente experimento se hizo un *traceroute* a la Universidad Estatal M.V. Lomonósov de Moscú, en Rusia.

En particular, se utilizó la *URL* `msu.ru` como dirección destino.

6.2. Motivación e Hipótesis

Es curioso preguntarse qué caminos encontraremos hacia Rusia, dado que en un principio pensamos estas posibilidades:

- El camino podría dirigirse directamente desde Argentina hacia Europa, atravesando dicho continente hasta llegar a Rusia, evidenciando un único salto intercontinental.
- El camino podría dirigirse a Estados Unidos, dado que la gran mayoría del tráfico pasa por allí, y luego cruzar directamente a Rusia por el pacífico.
- No descartamos que pueda haber una combinación de caminos entre Europa y Estados Unidos. De esta manera esperamos detectar con el método de *Cimbala* más de un salto intercontinental.

6.3. Análisis de Resultados

Obviaremos el *time exceeded* recibido del primer *ttl* debido a que es la respuesta que obtenemos del *router* correspondiente al lugar donde este experimento tuvo lugar[3], por lo cual no tiene mucha relevancia y no contribuye a mayor claridad en el experimento.

TTL	IP	RTT	Country	Continent	Cambió Cont. (Cimbala)	Cambió Cont. (Región IP)
2	*					
3	*					
4	*					
5	*					
6	200.89.161.97	0.12506	Argentina	América del Sur	No	No
7	200.89.165.197	0.11697	Argentina	América del Sur	No	No
8	200.89.165.222	0.12236	Argentina	América del Sur	No	No
9	190.216.88.33	0.11676	Argentina	América del Sur	No	No
10	67.17.99.233	0.24725	Estados Unidos	América del Norte	Sí	Sí
11	*					
12	4.69.158.245	0.36936	Estados Unidos	América del Norte	Sí	No
13	4.69.158.245	0.41262	Estados Unidos	América del Norte	No	No
14	213.242.110.198	0.46325	Gran Bretaña	Europa	No	Sí
15	*					
16	194.85.40.229	0.39466	Rusia	Asía	No	Sí
17	194.190.254.118	0.45311	Rusia	Asía	No	No
18	93.180.0.172	0.47593	Rusia	Asía	No	No
19	188.44.33.10	0.45023	Rusia	Asía	No	No
20	188.44.33.42	0.46457	Rusia	Asía	No	No
21	188.44.50.103	0.50492	Rusia	Asía	No	No

Cuadro 4: ICMP Traceroute a 188.44.50.103

Obtuvimos 5 *hosts* que no respondieron nuestros mensajes (24 %) y 16 que sí pudieron ser reconocidos (76 %).

El siguiente gráfico muestra uno de los posibles caminos tomados por el *traceroute*:

[3]Tienda del Cafe, Av. Santa Fe y Av. Callao

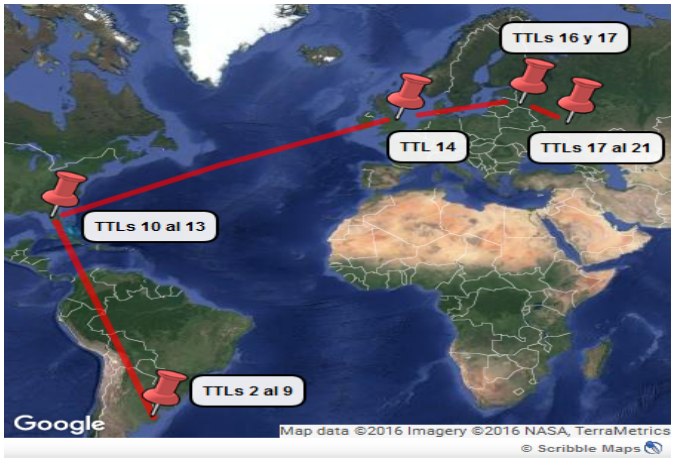

Figura 5: Posible camino tomado en el *traceroute*

6.4. Análisis general

Surguen varias cuestiones a la hora de analizar este *traceroute*:

- Los *hosts* correspondientes a los *TTLs* 2, 3, 4 y 5 no fueron encontrados. De todas maneras, el experimento fue hecho en el mismo lugar que el de Australia. Es interesante remarcar entonces que por más que ambos experimentos se realizaron desde el mismo lugar, como el destino era distinto, inmediatamente luego de haber pasado por el *router* del lugar los caminos tomados fueron distintos.
- Los *hosts* correspondientes a los *TTLs* 4, 5 y 6 pertenecen a Cablevisión S.A. No sabemos por qué una vez que ingresa por el *host* del *ttl* 4 los *rtts* empiezan a ser negativos.
- El *host* correspondiente al *ttl* 9 creemos que corresponde al *ISP (internet service provider)* de Cablevisión S.A. Este servicio es provisto por *Level 3 Communications, Inc.* empresa situada en Estados Unidos.
- El *host* correspondiente al *ttl* 10 efectivamente corresponde a *Level 3 Communications, Inc.*, por lo cual fue correctamente detectado el salto intercontinental por el método de *Cimbala*.
- A la hora de analizar el *host* del *ttl* 12 y 13 (son el mismo) surgen varias inquietudes:
  - La gran mayoría de las herramientas utilizadas para localizar las ips afirman que está situada en Estados Unidos. Sin embargo en algunos casos encontramos (en distintas páginas) que podría estar situada en Suecia o Alemania.
  - La primera vez que se llega al *host* hay una diferencia importante entre los *rtts*, lo cual sugiere que ha ocurrido un salto intercontinental. Esto reforzaría la probabilidad de los casos encontrados por fuera de Estados Unidos, además de que es confirmado a su vez por el método de *Cimbala*.
  - No pudimos sacar ninguna conclusión respecto de por qué para ambos *ttls* el host era el mismo. Particularmente como todas las veces que se realizó el experimento sucedió eso, descartamos el hecho de que pudieran haber sido distintas rutas por las cuales a veces se pasaba por ese *host* con *ttl* 4 y a veces con 5.
- El *host* correspondiente al *ttl* 14 también es confuso de analizar. La diferencia de *rtts* no presenta evidencia de un salto intercontinental, pero suponiendo que en realidad los *hosts* anteriores no estaban efectivamente en Estados Unidos, podría ser que tenga más sentido. Otras aplicaciones muestran que la ip pertenece a Stockholm, Suecia, Connaught, Irlanda, o Francia. En seguida hipotetizaremos de por qué quizás tenga sentido que en el host de *ttl* 13 haya sucedido un salto intercontinental y que la ruta tomada haya sido por Suecia.
- El *host* correspondientes a los *ttls* 16 y 17 ya pertenecen a Rusia, Saint Petersburg City. La razón por la cual creemos que los nodos pertenecientes a los *ttls* 12 y 14 podrían haber pertenecido a Suecia es porque siguen perteneciendo a la ruta provista por *Level 3 Communications, Inc.* y

podemos ver en su mapa de redes[4] que tienen una ruta hasta Stockholm Suecia, a partir de donde se pasa a utilizar una ruta pública que se dirige hacía Rusia, pasando por la ciudad previamente mencionada.

- A partir del *ttl* 18 se ingresa a Moscú, donde se encuentra la universidad que estabamos buscando.

Los siguientes gráficos muestran la diferencia relativa de *rtts*, ademas de los datos utilizados por el algoritmo de *Cimbala* para detectar *outliers*:

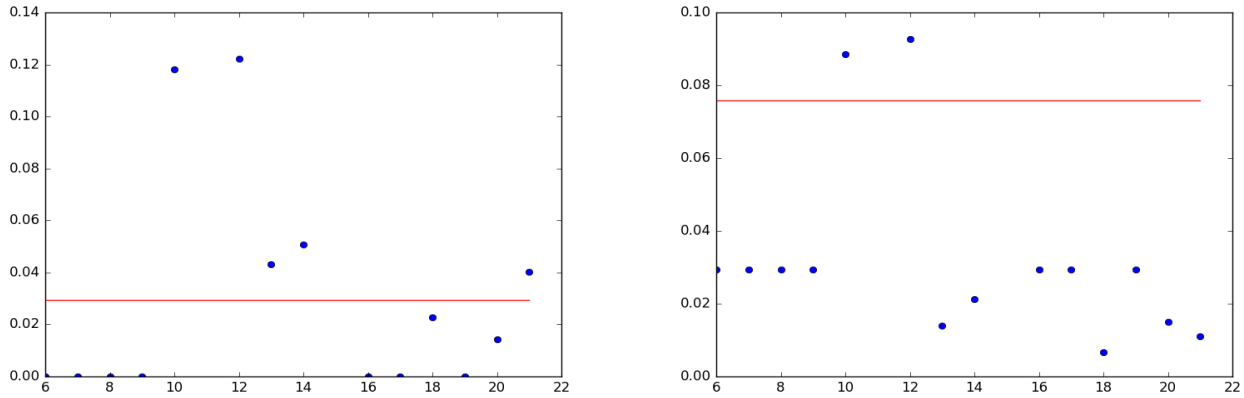

Figura 6: A la izquierda, la diferencia relativa de *rtts*. A la derecha, los datos utilizados por el método de *Cimbala* para detectar *outliers*

Podemos notar en ambos gráficos como los *hosts* donde es más probable que hayan ocurrido los saltos intercontinentales fueron en los *ttls* 10 y 12. Esto refuerza nuestra teoría de que efectivamente en el *ttl* 12 ya se ingresó a la región de Europa, dado que luego llegar a Rusia (*ttl* 16 y 17) no presenta ninguna diferencia significativa de tiempo.

El siguiente gráfico muestra el camino alterno sobre el cual hipotetizamos previamente:

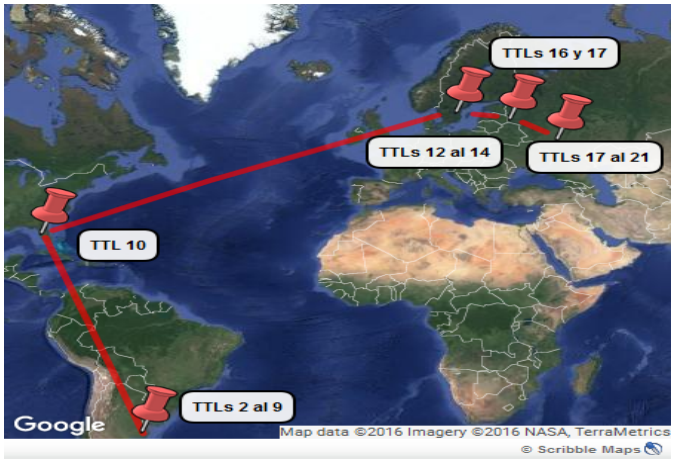

Figura 7: Posible camino tomado en el *traceroute*

Según nuestra hipótesis, el método de *Cimbala* pudo evidenciar todos los saltos intercontinentales. No tenemos en cuenta el traslado de Europa a Asia dado que no hay mucha distancia a recorrer allí. Además, aquellos saltos no intercontinentales no fueron reconocidos como *outliers* por el algoritmo.

[4] `http://www.level3.com/~/media/files/maps/en-network-services-level-3-network-map.pdf`

7. Cuarto Experimento: Japón

7.1. Presentación

En el siguiente experimento se hizo un *traceroute* a la univerdiad de Tokyo, Japón.
En particular, se utilizó la *URL* `www.u-tokyo.ac.jp` como dirección destino.

7.2. Motivación e Hipótesis

La motiviación de esta ubicación fue buscar una universidad que se encuentre en el otro hemisferio y separada por un gran océano como es el pacífico, para que de este modo podamos ver si se utilizan rutas sobre el pacífico o bien se hacen pasos intermedios por África o Europa para llegar a Asia.

Creemos que podrían darse los siguientes casos:

- Podría ir de Argentina a Chile y desde ahí cruzar el océano pacífico hasta Australia y luego subir hasta Japón.
- Podría ir por América hasta el Norte y de ahí saltar a Asia.
- Podría ir por América hasta el Norte y de ahí saltar a Europa y luego Asia.
- Podría ir a África y luego Asia.

7.3. Análisis de Resultados

Obviaremos el *time exceeded* recibido del primer *ttl* debido a que es la respuesta que obtenemos del *router hogareño* correspondiente a la casa de uno de los integrantes situada en San Martín.

TTL	IP	RTT	Country	Continent	Cambió Cont. (Cimbala)	Cambió Cont. (Región IP)
2	200.3.60.191	0,0381	Argentina	Sudamérica	No	No
3	181.88.145.142	0,1685	Argentina	Sudamérica	Si	No
4	200.3.37.234	0,1675	Argentina	Sudamérica	No	No
5	198.32.124.176	0,1664	USA	Norteamérica	No	Si
6	184.105.213.25	0,1886	USA	Norteamérica	No	No
7	184.105.81.201	0,2068	USA	Norteamérica	No	No
8	184.105.64.150	0,2147	USA	Norteamérica	No	No
9	184.105.223.193	0,2710	USA	Norteamérica	No	No
10	184.105.213.118	0,3730	USA	Norteamérica	No	No
11	184.105.81.26	0,3736	USA	Norteamérica	No	No
12	*					
13	124.83.252.242	0,4922	Japón	Asia	No	Si
14	158.205.134.22	0,4756	Japón	Asia	No	No
15	*					
16	*					
17	*					
18	154.34.240.254	0,4853	Japón	Asia	No	No
19	210.152.135.178	0,4846	Japón	Asia	No	No

Cuadro 5: ICMP Traceroute a 210.152.135.178

Obtuvimos 4 *hosts* que no respondieron nuestros mensajes (22 %) y 14 que sí pudieron ser reconocidos (88 %).

El siguiente gráfico muestra uno de los posibles caminos tomados por el *traceroute*:

Figura 8: Posible camino tomado en el *traceroute*

7.4. Análisis general

Surgen varias cuestiones a la hora de analizar este *traceroute*:

- Los *hosts* correspondientes a los *TTLs* 2, 3 y 4 corresponden al ISP, en este caso Telecom y el primero se encuentra en Palermo, Capital Federal y los siguientes dos en Entre Ríos. Podemos ver que el mayor incremento de rtt fue aquí y no fue un salto intercontinental. No tenemos forma de asegurar cuál es el causante pero creemos que puede ser originado por una limitación del enlace entre Bs. As. y Entre Ríos o bien una congestión alta del router de Entre Ríos que genera una demora en los paquetes.

- El *host* correspondientes al *TTL* 5 es el primer salto intercontinental, ya que desde Argentina a Estados Unidos viaja en un sólo salto, y no sólo que la diferencia con el salto anterior en rtt no es mucho mayor sino que, contrario a lo esperado, fue menor. Como hemos mencionado antes es probable que la causa sea que ciertos routers manejan distintas colas de prioridades para los paquetes ICMP. Su ubicación es Miami.

- Entre los *TTL* 6 y el 11 las ips asociadas pertenecen a la empresa *Hurricane Electric* y la mayoría de los geolocalizadores de IP proponen a *Fremont, California* como ubicación, algo que no resulta demasiado lógico. Analizando varias fuentes encontramos que sólo algunos resultados, en menor proporción, ubicaron al TTL 6 en *Kansas*, 7 en *Fremont, California*, 8 en *Taipei, Taiwan*, el 9 nuevamente *Fremont, California* y por último el 10 y 11 están ubicados en *Tokyio, Japón*. Por no ser la información que más preponderante fue que dejamos USA en todos los casos pero esto explicaría la diferencia de *RTT* entre 8 y 9 y también entre 9 y 10.

- Los hosts correspondientes a los *ttl* del 13 en adelante se encuentran en Tokyo y mantienen el mismo *rtt*, siendo el 13 mayor al resto, probablemente por las prioridades a los mensajes ICMP. De cierta manera estos *hosts* podrían contrastar lo previamente dicho, ya que se evidencia una diferencia significativa de *rtt* al llegar a Japón en el *ttl* 13, desmereciendo la hipótesis de que en el *ttl* 10 ya se podría haber llegado.

Los siguientes gráficos muestran la diferencia relativa de *rtts*, ademas de los datos utilizados por el algoritmo de *Cimbala* para detectar *outliers*:

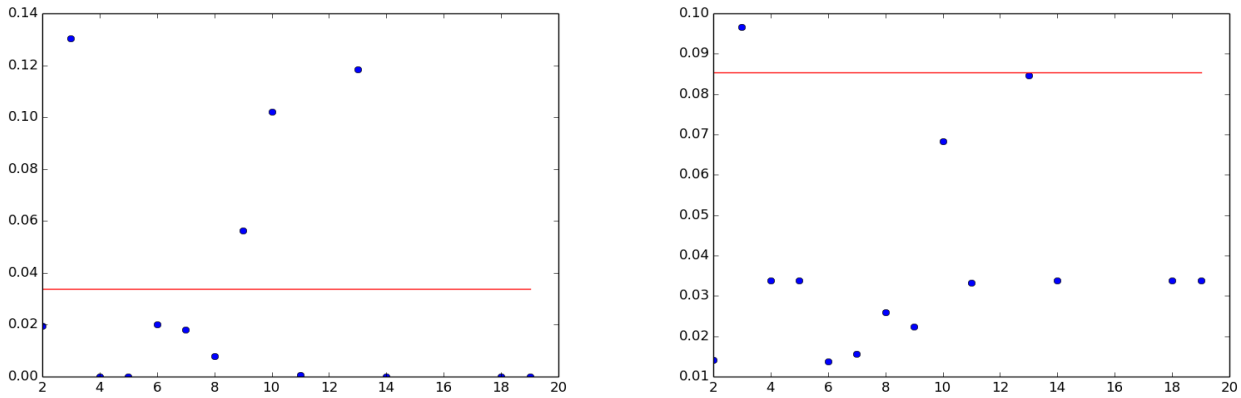

Figura 9: A la izquierda, la diferencia relativa de *rtts*. A la derecha, los datos utilizados por el método de *Cimbala* para detectar *outliers*

Tal como comentabamos antes, el ttl 3 sigue como outlier por la grán diferencia que hay entre dicho salto y el anterior. Si uno mira sólo el gráfico de la diferencia de rtt, el ttl 9 pareciera tener cierto grado de significancia por encima de la media pero viendo el de *Cimbala* claramente no es un *outlier*. El ttl 10 respalda la teoría del salto a Japón que suponemos entre el salto 9 y 10. Y por último el ttl 13 podemos estar 100 % seguros que es un salto intercontinental y por 0,001 no se tomó como outlier.

8. Conclusiones

Por más que el método teórico de *Cimbala* funcionó en la mayoría de los casos, pudimos ver como en la vida real hay muchas variables que se escapan del control y pueden meter ruido:

- Routers que le dan mas prioridad a un tipo de paquetes que a otros.
- Congestión.
- Que no sea determinística la ruta que va a tomar un paquete.
- Diferencias negativas de *rtt* a lo largo del camino.

Aunque el método funcione como una herramienta util para detectar o alertar sobre ciertas cosas, sigue siendo necesario el análisis particular de los datos para poder afirmar o contrastar hipótesis.