DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico II

Segundo cuatrimestre 2016 — Teoría de las comunicaciones

Integrante	LU	Correo electrónico
Oller, Luca	667/13	ollerrr@live.com
Zamboni, Gianfranco	219/13	gianfranco376@gmail.com
González, Rodrigo	294/01	rodrigogk@gmail.com

Palabras clave

traceroute outliers

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) 4576-3300
http://www.exactas.uba.ar

Índice

1. Introducción

El objetivo de este trabajo práctico es experimentar con herramientas y técnicas de uso frecuente a nivel de red, la versión de traceroute basada en los mensajes echo request/reply del protocolo ICMP. Para lograr esto se implementará una herramienta con la que se envían sucesivos paquetes con TTLs incrementales, calculando los RTTs entre cada salto y analizando la existencia de saltos intercontinentales.

Luego se analizarán, utilizando nociones de estadística, las rutas de los paquetes que enviaremos a universidades ubicadas en diferentes lugares del mundo.

2. Implementación de la herramienta

Para poder llevar a cabo de manera satisfactoria los experimentos, se implementó una herramienta que permita realizar un traceroute enviando paquetes con TTLs incrementales, obteniendo métricas (como el RTT de cada envío) y, a través de la técnica propuesta por Cimbala, se intentó detectar enlaces intercontinentales. De está forma, se facilitó, además, la comparación y procesamiento de dichos datos y se pudo llegar a conclusiones de una manera rápida e intuitiva.

Dicha herramienta fue desarrollada en Python (traceroute.py) y se puede ejecutar por línea de comando. La misma permite una serie de parametrizaciones mediante la cual es posible indicar:

- Destino: URL o IP
- Máximo TTL: cantidad de saltos que se van a intentar (si se alcanza el destino antes, se detiene la ejecución).
- Timeout por TTL: tiempo de espera máximo para recibir una respuesta.
- Mediciones por TTL: cantidad de veces que repetimos el envío para un TTL determinado.
- Intentos por TTL: cantidad de reintentos que se realizan si no se obtiene una respuesta
- Método utilizado para el cálculo de outliers: Cimbala standard o Cimbala en varios pasos.

Para nuestros experimentos hemos utilizado: 30 TTL como máximo, 0.3 segundos de timeout, 30 mediciones por TTL y 3 reintentos. En cuanto al método utilizado para detectar outliers probamos las dos alternativas: detectar outliers en una primera pasada o en varias pasadas (eliminando un outlier cada paso y volviendo a ejecutar el algoritmo de detección). Nos quedamos con la primera opción (una única pasada) ya que el segundo método arrojaba una gran cantidad de falsos positivos para nuestros experimentos.

La determinación del RTT se hizo en base al tiempo transcurrido desde que se envía un paquete y se recibe.

```
t_inicial = time.perf_counter()
respuesta = scapy.sr1(paquete,timeout)
rtt = time.perf_counter() - t_inicial
```

3. Experimentación

Hemos seleccionado tres universidades ubicadas en distintos continentes para realizar nuestros experimentos:

- Cape Peninsula University of Technology(CPUT), Sudáfrica, www.cput.ac.za
- Jagiellonian University(UJ), Polonia, www.en.uj.edu.pl
- Universidad de Teikyo, Japón, www.teikyo-u.ac.jp

Esta selección es el resultado de varias pruebas efectuadas sobre un conjunto mayor de universidades. Nos hemos quedado con estas tres porque los destinos eran alcanzables por nuestra herramienta y había una cantidad de saltos considerables para realizar los análisis posteriores. Hubo un subconjunto de casos en los que el destino no era alcanzado. No conocemos con precisión el porqué a partir de cierto salto, no se obtenían más respuestas. Posiblemente, de acuerdo al documento "Traceroute Anomalies (Jobst)"nos hemos topado con destinos protegidos por un firewall.

A continuación, mostraremos los resultados obtenidos. Para la realización de los gráficos a partir del output conseguido con nuestra herramienta, se utilizó Google Maps y Plot.ly. Para geolocalizar, utilizamos www.geoiptool.com/es/ e ip-api.com.

4. Resultados

4.1. Sudáfrica - Cape Peninsula University of Technology: CPUT

Como primer caso a experimentar con nuestra herramienta decidimos analizar la ruta obtenida hasta llegar a una universidad sudafricana (www.cput.ac.za).

Obtuvimos los siguientes resultados:

Cuadro 1: Información obtenida.

TTL	Hop	RTT promedio	Continente	Outlier
1	192.168.0.1	55ms	SA	
2	10.18.128.1	62ms	SA	
3	10.242.0.17	64ms	SA	
4	195.22.220.33	65ms	SA	
5	195.22.220.32	64ms	SA	
6	89.221.41.181	186ms	NA	X
7	89.221.41.161	189ms	NA	
8	154.54.9.17	192ms	NA	
9	154.54.80.41	188ms	NA	
10	154.54.24.193	203ms	NA	
11	154.54.7.157	211ms	NA	
12	154.54.40.105	214ms	NA	
13	154.54.30.186	284ms	NA	
14	154.54.58.174	283ms	NA	
15	154.54.56.242	275ms	NA	
16	149.14.80.210	274ms	NA	
17	196.32.209.174	217ms	AF	
18	155.232.6.65	231ms	AF	
19	155.232.6.205	208ms	AF	
20	196.21.74.34	120ms	AF	X
21	196.21.76.18	210ms	AF	
22	198.54.223.213	192ms	AF	

Para esta medición, originalmente nos daba que los saltos 4 y 5 pertenecían a Europa. Chequeando en otras fuentes(http://www.my-address-ip.com/whois-address-ip-195.22.220.33.html) vimos que la IP era de Argentina. Ésto tiene sentido porque el tiempo de RTT promedio es similar al de los primeros hops y es bastante menor al europeo.

Resultados:

- Todos los saltos respondieron los time exceeded.
- La ruta tiene 22 saltos
- La ruta presenta 2 saltos intercontinentales: de Sudamérica a Norteamérica y de Norteamérica a África.
- La distribución de RTT presenta outliers según el método de Cimbala.
- El primer enlace intercontinental es detectado por el método de outliers. Un segundo enlace es predicho, pero no es detectado con precisión. Se podría decir que habría un falso positivo (el que detectó en forma incorrecta) y un falso negativo (el que no detectó).

El siguiente mapa muestra los tramos intercontinentales:

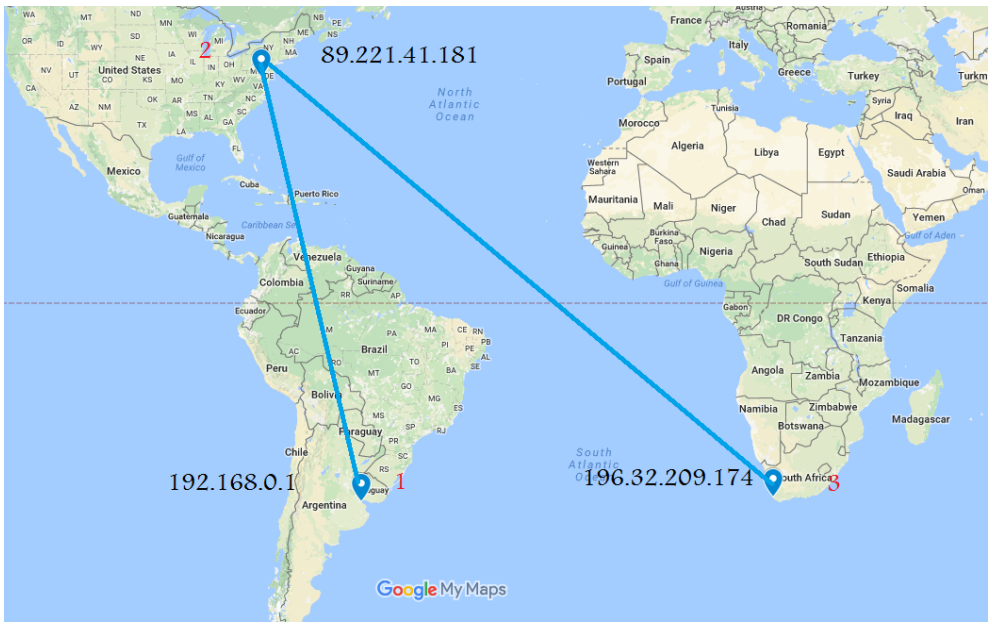

Figura 1: Ubicación de los enlaces intercontinentales para el traceroute a www.cput.ac.za

Podemos observar los dos saltos intercontinentales entre Sudamérica y Norteamérica, y de Norteamérica a África.

A continuación tenemos el gráfico con las diferencias de RTT entre saltos.

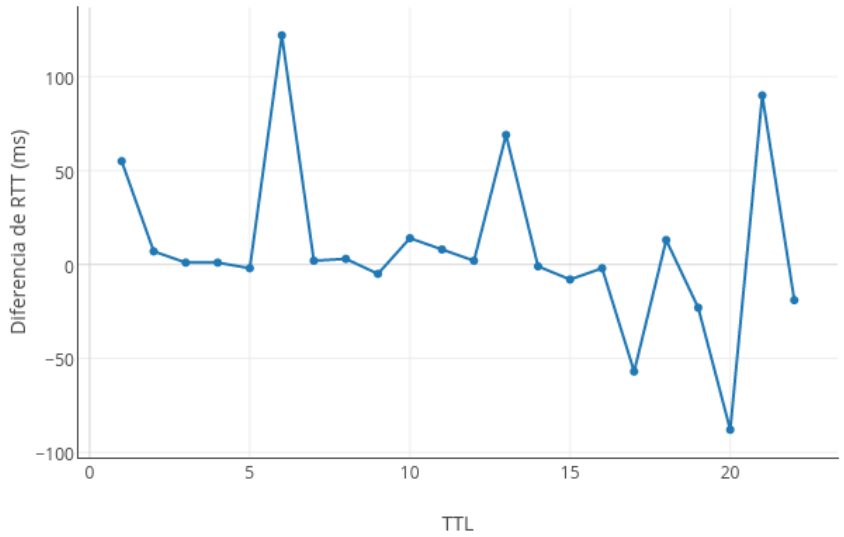

Figura 2: Diferencia de RTT entre saltos para el traceroute a www.cput.ac.za

Podemos observar que una correspondencia entre el primer pico del gráfico (en TTL = 6) con la presencia de un enlace intercontinental. Luego, no encontramos la correspondencia con el segundo enlace intercontinental.

El siguiente gráfico muestra el valor Z:

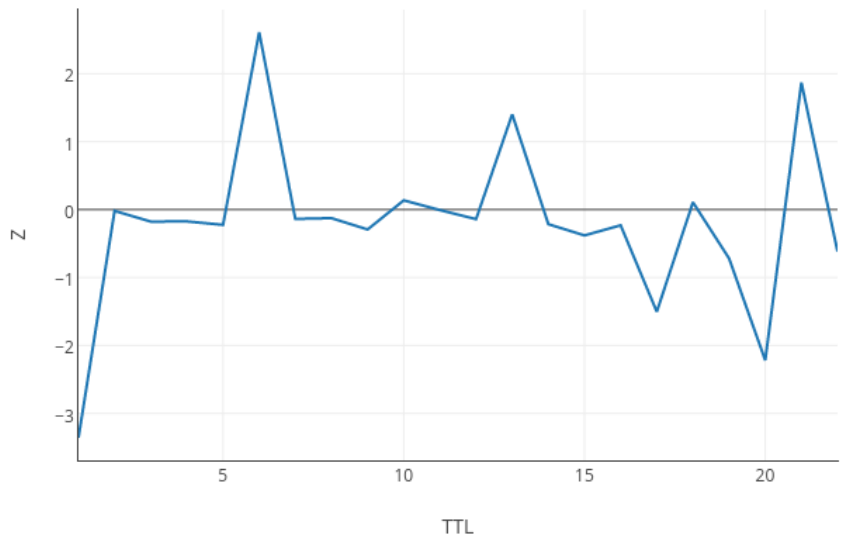

Figura 3: Cálculo del valor Z para el traceroute a www.cput.ac.za

Podemos notar que para el TTL=6 donde se presenta el enlace intercontinental, el valor de la función alcanza el pico máximo.

4.2. Polonia- Jagiellonian University - UJ

Nuestro segundo caso de estudio fue la Universidad de Jagiellonian (www.en.uj.edu.pl). Para hacerlo corrimos el script de python y obtuvimos los siguientes resultados:

Cuadro 2: Información obtenida.

TTL	Hop	RTT promedio	Continente	Outlier
1	192.168.0.1	56ms	SA	
2	10.18.128.1	65ms	SA	
3	10.242.0.17	64ms	SA	
4	208.178.195.210	70ms	NA	
5	208.178.195.209	63ms	NA	
6	*	*	*	
7	4.69.161.6	303ms	NA	X
8	4.69.161.6	273ms	NA	
9	212.162.10.82	298ms	EU	
10	212.191.224.70	315ms	EU	
11	149.156.0.54	316ms	EU	
12	149.156.76.2	316ms	EU	
13	149.156.89.10	318ms	EU	
14	149.156.225.217	313ms	EU	

Resultados:

- No todos los saltos respondieron el time exceeded (para TTL = 6 no obtuvimos respuesta)
- La ruta tiene 13 saltos (en término de saltos que sí responden)

- La ruta presenta 2 saltos intercontinentales: de Sudamérica a Norteamérica y de Norteamérica a Europa.
- La distribución de RTT presenta outliers según el método de Cimbala
- No se detectaron con precisión los saltos intercontinentales

El siguiente mapa muestra los tramos intercontinentales:

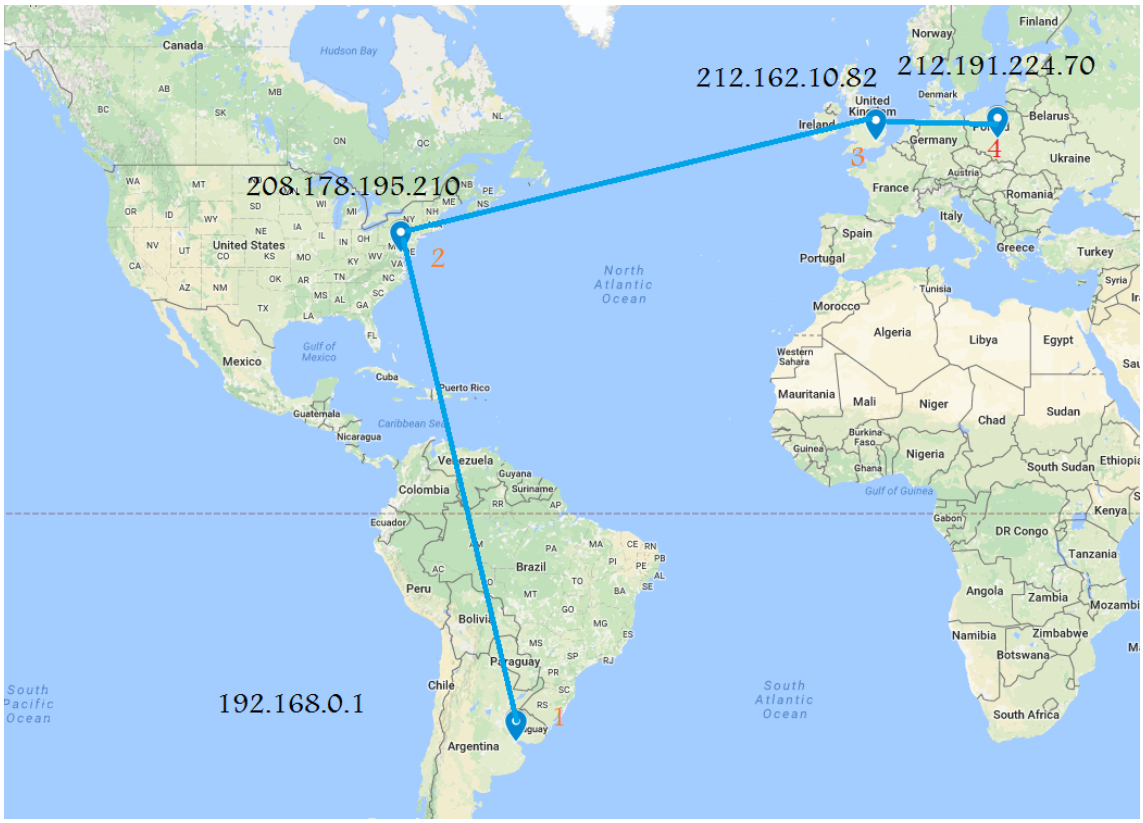

Figura 4: Ubicación de los enlaces intercontinentales para el traceroute a www.en.uj.edu.pl

Si bien Inglaterra y Polonia están en el mismo continente, es interesante notar que el salto desde América del Norte hacia Europa se da primero en a un país más cercano de la parte oeste del continente y luego a Polonia que pertenece a Europa Oriental.

A continuación tenemos los gráficos con las diferencias de RTT entre saltos y el valor Z.

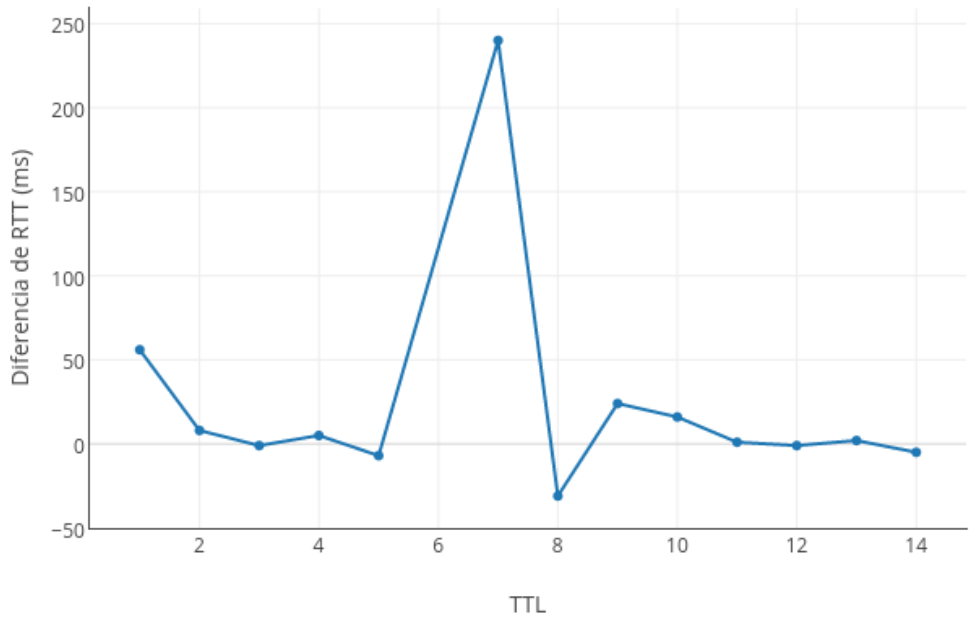

Figura 5: Diferencia de RTT entre saltos para el traceroute a www.en.uj.edu.pl

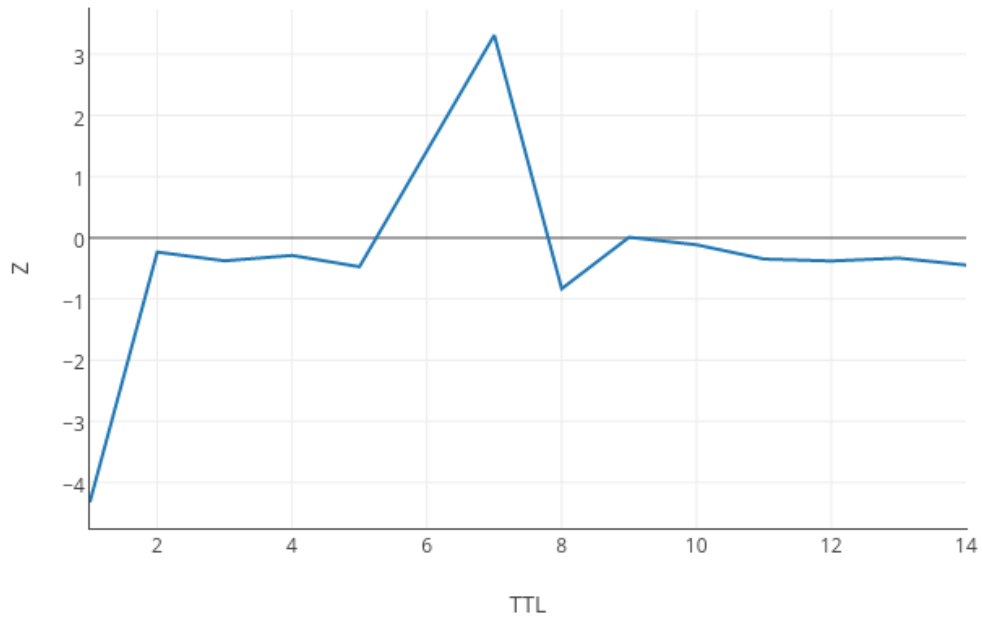

Figura 6: Cálculo del valor Z para el traceroute a www.en.uj.edu.pl

Podemos notar un pico pronunciado en ambas gráficas que denotan la presencia de un enlace inter-

continental. Sin embargo, no coincide precisamente en el hop que se esperaba.

4.3. Japón- Universidad de Teikyo

Para el tercer experimento, decidimos ir a Japón, a Teikyo (www.teikyo-u.ac.jp). Los resultados fueron los siguientes:

Cuadro 3: Información obtenida.

TTL	Hop	RTT promedio	Continente	Outlier
1	192.168.0.1	63	SA	
2	10.18.128.1	64	SA	
3	10.242.0.17	69	SA	
4	208.178.195.210	68	NA	
5	208.178.195.209	68	NA	
6	67.17.111.65	237	NA	X
7	64.208.27.114	219	NA	
8	203.181.106.13	210	AS	
9	59.128.3.178	215	AS	
10	203.181.100.117	334	AS	
11	118.155.197.53	278	AS	
12	118.159.225.14	319	AS	
13	203.140.224.106	253	AS	
14	203.140.225.82	321	AS	
15	14.128.31.106	314	AS	
16	14.128.19.30	319	AS	
17	112.140.52.105	334	AS	

Resultados:

- Todos los saltos respondieron el time exceeded
- La ruta tiene 17 saltos
- La ruta presenta 2 saltos intercontinentales: de Sudamérica a Norteamérica y de Norteamérica a Asia.
- La distribución de RTT presenta outliers según el método de Cimbala
- No se detectaron con precisión los saltos intercontinentales

El siguiente mapa muestra los tramos intercontinentales:

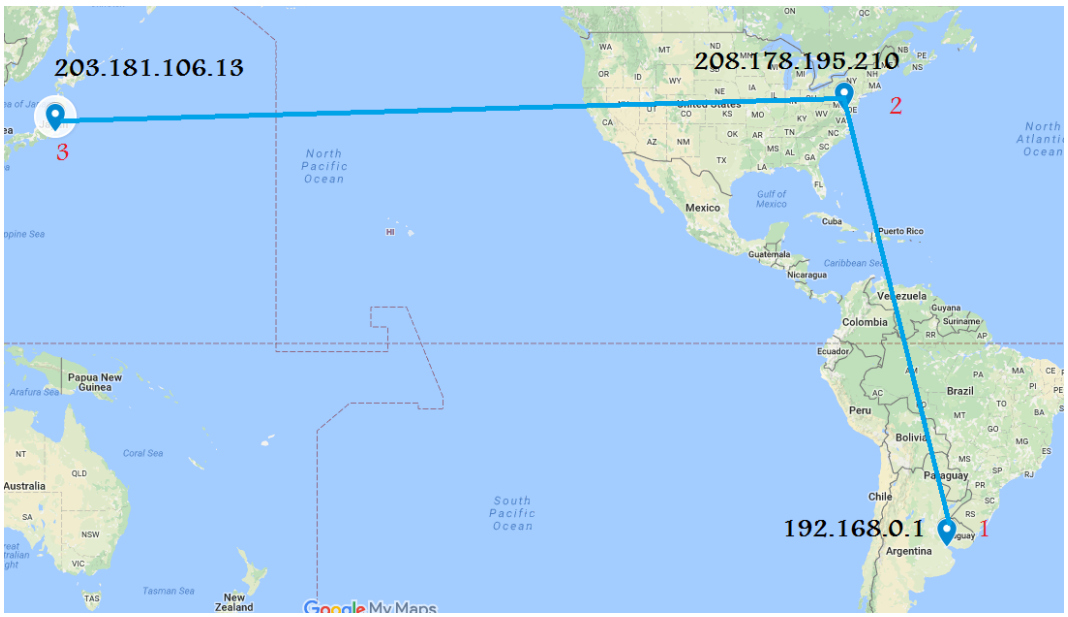

Figura 7: Ubicación de los enlaces intercontinentales para el traceroute a www.teikyo-u.ac.jp

Podemos observar un salto entre Sudamérica y Norteamérica, y otro salto entre Norteamérica y Asia. A continuación, los gráficos con la diferencia de RTT y el valor Z entre saltos:

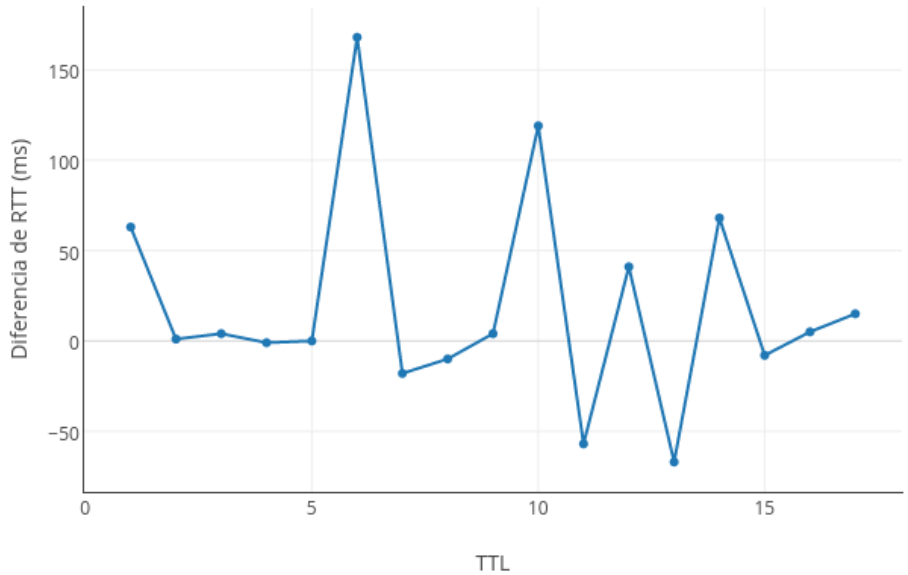

Figura 8: Diferencia de RTT entre saltos para el traceroute a www.teikyo-u.ac.jp

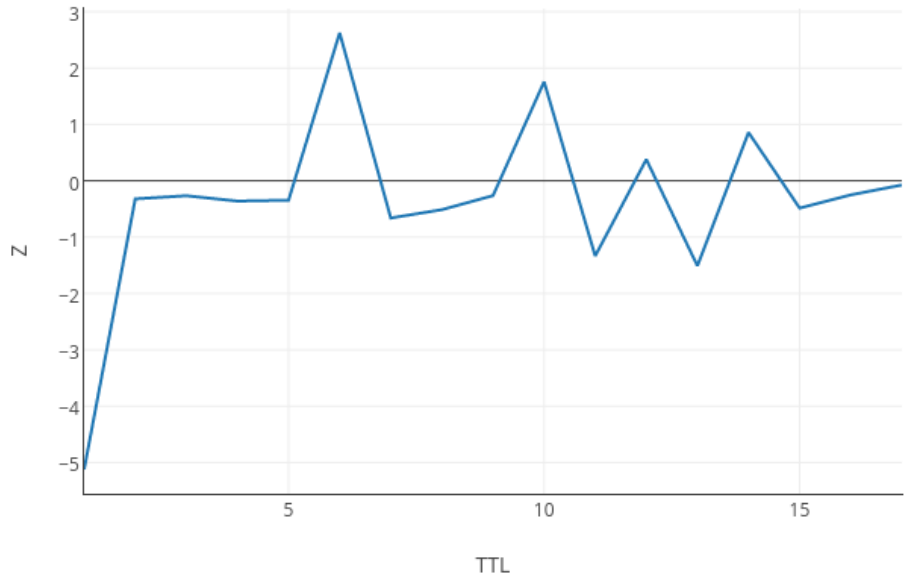

Figura 9: Cálculo del valor Z para el traceroute a www.teikyo-u.ac.jp

Podemos detectar la presencia de enlaces intercontinentales por observación de las variaciones del valor Z en el gráfico, aunque no se determina con precisión en qué salto se produce.

5. Conclusiones

El presente trabajo nos ha acercado al manejo de herramientas que eran desconocidas hasta el momento para nosotros. Ha sido interesante trabajar con la manipulación de paquetes y poder desarrollar una implementación propia de una herramienta tan utilizada como el traceroute.

Durante los experimentos realizados hemos encontrado algunas anomalías, como por ejemplo: la no respuesta de un paquete ICMP. Esta no respuesta se dio de dos maneras: para un TTL determinado no obtuvimos respuesta o bien, dejamos de obtener respuesta a partir de un TTL. En el primer caso, de acuerdo al documento de Jobst, podemos inferir que nos topamos con un link (router) que está configurado para no responder los mensajes ICMP que alcanzan un valor TTL = 0 (aunque sí, forwardea los paquetes al siguiente hop). En la segunda situación, podemos decir que nos topamos con un link que tenía una configuración de firewall que no permitió que el paquete pasara al siguiente link.

Otro punto interesante que notamos es que los RTT no fueron incrementales como esperábamos. En teoría el valor de RTT debería ser creciente a medida que aumenta el valor de TTL, sin embargo, en la práctica notamos que ésto no fue así. De acuerdo al documento de Jobst, ésto es una anomalía, y puede responder a diversas situaciones: el camino de regreso de los paquetes puede ser diferente al de ida (tal vez, la vuelta es más rápida desde un router más lejano), o bien hay control de tráfico en los routers intermedios, configurados con prioridades para forwardear rápidamente un paquete, pero tardando para responder ante un TTL = 0.

Estas anomalías, ensucian el conjunto de resultados, y hace que la predicción de determinadas situaciones (como la presencia de enlaces intercontinentales) no se correspondan en la práctica con lo que dice la teoría.

En este escenario, no podemos mejorar las predicciones de los enlaces usando un valor de corte fijo para el valor de Z. Obviamente, que si usamos un valor de corte bajo, vamos a encontrar mayor cantidad de outliers, pero muchos van a ser falsos positivos. Si no existieran anomalías, y los RTT fueran proporcionales a la distancia recorrida, seguramente detectaríamos fácilmente los enlaces intercontinentales (porque serían largas distancias recorridas). Un método más efectivo, a nuestro parecer, es el de geolocalizar direcciones IP. En ese caso sería simple encontrar esos enlaces transoceánicos (ante un cambio de continente). Sin embargo, para este trabajo práctico, no encontramos una fuente confiable para tal tarea, ya que muchas de las direcciones IP consultadas arrojaron resultados incorrectos.