DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

TP2: Rutas en Internet

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Furman, Damián	936/11	damian.a.furman@gmail.com
Lambrisca, Santiago	274/10	santiagolambrisca@hotmail.com
Marottoli, Daniela	42/10	dani.marottoli@gmail.com
Vanecek, Juan	169-10	juann.vanecek@hotmail.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

Contents

1 Introducción

Este trabajo práctico fue realizado con el objetivo de entender el protocolo ICMP y de implementar nuestra propia herramienta de traceroute utilizando este protocolo de control, para finalmente poder realizar un analisis sobre los resultados obtenidos que nos permita entender un poco mejor que es lo que realmente sucede.

En primer lugar se seleccionaron cuatro universidades situadas en diferentes continentes. Una de ellas es The University of British Columbia, ubicada en la ciudad de Vancouver en Canadá. La segunda es The University of Hong Kong, ubicada en Pokfulam, Hong Kong. Otra de las universidades seleccionadas es Lomonosov Moscow State University, ubicada en Moscú, Rusia. La ultima es The National University of Samoa.

La primera parte del trabajo consiste en implementar una herramienta que nos permita estimar el $RountTripTime$ entre nuestro host y distintos hosts, calculando además el $valorstandard$ de cada salto con respecto a la ruta global.

Luego, procedemos a gráficar y analizar los resultados obtenidos, intentando reconocer enlaces submarinos. Se tendra en cuenta para esto el $valorstandard$ calculado por nuestra herramienta y se intentara encontrar un umbral que permita decidir de manera lo suficientemente acertada cuales son los enlaces submarinos.

2 Desarrollo

La implementación de nuestra herramienta consiste principalmente en una clase, la cual cuenta con los métodos necesarios para realizar el envio de paquetes $ICMP$ a un host dado, recibir las respuestas, y calcular cuál es el tiempo entre el envío y la recepción de una respuesta, y estimar cuál fue la ruta de los paquetes.

Para poder estimar la ruta de los paquetes hasta el destino, la estrategia utilizada será incrementar el valor del campo *ttl* en 1, así empezando con un $ttl = 1$ iremos obteniendo una respuesta $ICMP$ de tipo *timeexceeded* para cada salto. De esta manera, iremos guardando la informacón obtenida para cada valor del *ttl*, y rastreando la ruta de los paquetes.

Debido a que en cada medición los resultados obtenidos presentan variaciones, lo que hacemos es estimar los tiempos obtenidos realizando un promedio sobre cada tiempo. Por lo tanto, enviaremos más de un paquete por *ttl*, con el objetivo de evitar malas estimaciones causadas por cirscunstancias extraordinarias en un instante dado.

Por otro lado, utilizaremos herramientas de geolocalización, que nos permiten estimar la ubicación de los routers a través de los cuáles se fordwardearon los paquetes y dibujar su recorrido en un mapa. Esto es de gran utilidad a la hora de corroborar qué saltos se corresponden con enlaces submarinos.

Nuestra herramienta nos permite correr el algoritmo para distintos destinos, cambiando la cantidad de paquetes por ttl, el umbral y tambien la herramienta de geolocalización utilizada, para asi poder tener una mayor cantidad de posibilidades a la hora de experimentar. Además se implemento una herramienta de control de ejecución, la cual nos permite correr el algoritmo cada cierto intervalo de tiempo, y tener resultados para distintos momentos del día. Nosotros utilizaremos intervalos de 1 hora.

Los resultados son almacenados en archivos de texto, para poder contar con la información a la hora de graficar y analizar los resultados.

3 Resultados

A continuación presentaremos los distintos gráficos y analisis realizados, en relacion a las 4 universidades elegidas. Merece nombrarse, que se habia elegido una universidad más, llamada University of Pretoria.

En cuanto a esta ultima universidad nombrada, nos encontramos con que no pudimos rastrear su ruta. Lo que obtuvimos en nuestros intentos, fue siempre el mismo resultado. Incrementamos el *ttl* hasta obtener un *ubyte* overflow. El valor de nuestro *ttl* se fue del rango $0 < ttl < 255$. Por este motivo no utilizamos este caso de estudio en los gráficos y analisis.

3.1 Selección de las universidades

Las 4 universidades de distintas partes del mundo seleccionadas para llevar a cabo el análisis requerido son las siguientes:

- **The University of British Columbia**

  Distancia: 11302.14 km

  IP: 137.82.130.49 (`www.ubc.ca`)

- **Lomonosov Moscow State University**

  Distancia: 13481.01 km

  IP: 93.180.0.18 (`www.msu.ru`)

- **The Chinese University of Hong Kong**

  Distancia: 18511.04 km

  IP: 137.189.11.73 (`www.cuhk.edu.hk`)

- **National University Of Samoa**

  Distancia: 10771.06 km

  IP: 23.229.137.67 (`www.nus.edu.ws/`)

Las distancias descriptas corresponden a la distancia lineal que hay entre la universidad y un punto en común en Buenos Aires.

3.2 Primera Parte: Correr nuestro Traceroute

Se ejecutó el traceroute implementado por nosotros utilizando Scapy a lo largo de un día, con intervalos de una hora. El traceroute envía 20 paquetes a cada hop, para lograr un promedio más ajustado del RTT.

Evaluamos distintas herramientas de geolocalización para calcular las coordenadas y/o la localización de las IP's con el objetivo de que nuestros datos sean lo más precisos posibles.

Los resultados obtenidos se muestran en tres gráficos distintos por cada universidad, cada uno representando una ejecución diferente del algoritmo de *traceroute* desde una máquina distinta (por eso difieren con mayor grado la o las primeras IP's que devuelve el algoritmo) en la cual se utilizó una API de geolocalización distinta. En cada gráfico hay una línea por cada hora en la que se ejecutó el traceroute marcando los distintos valores de los RTT's en función de los TTL's. A continuación se muestran los gráficos:

Para todas las API's se puede observar un aumento considerable del RTT entre dos TLL's específicas (distintas según cada gráfico) que representa una transmisión de gran escala.

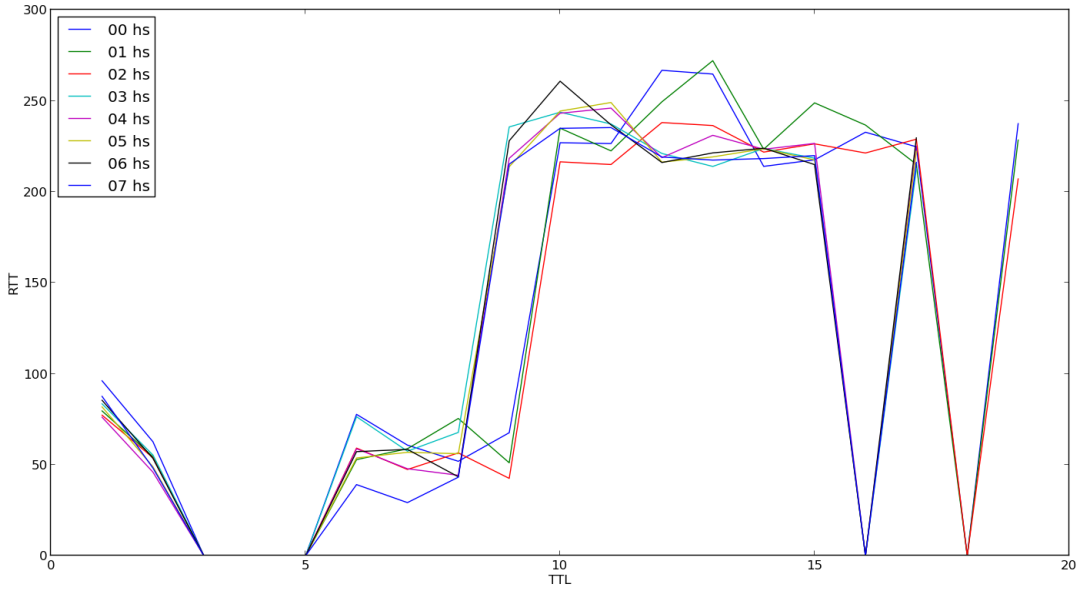

Figure 1: Canada Muestra 1

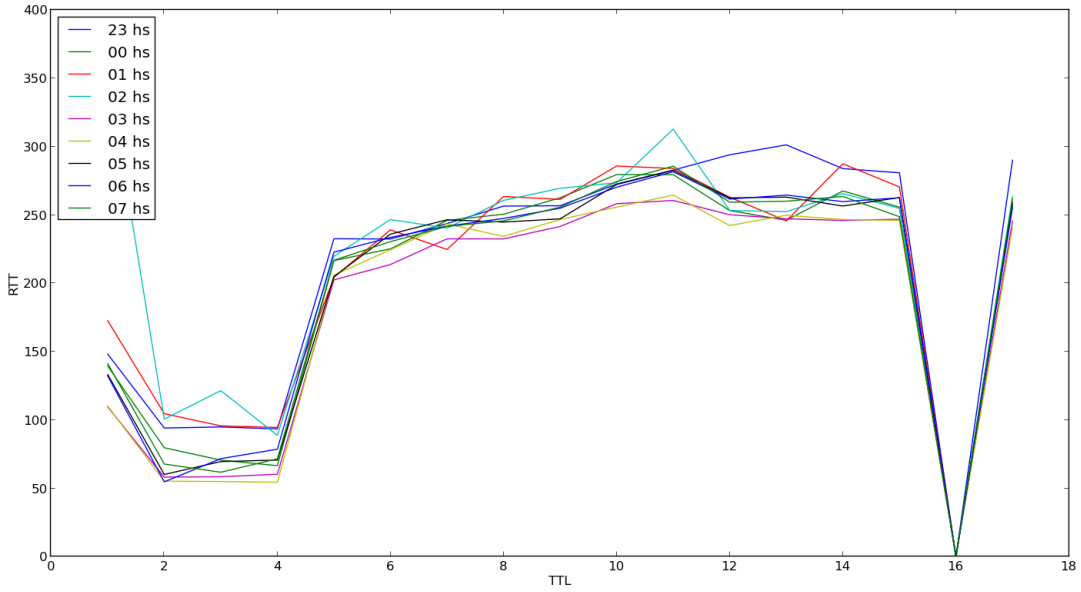

Figure 2: Canada Muestra 2

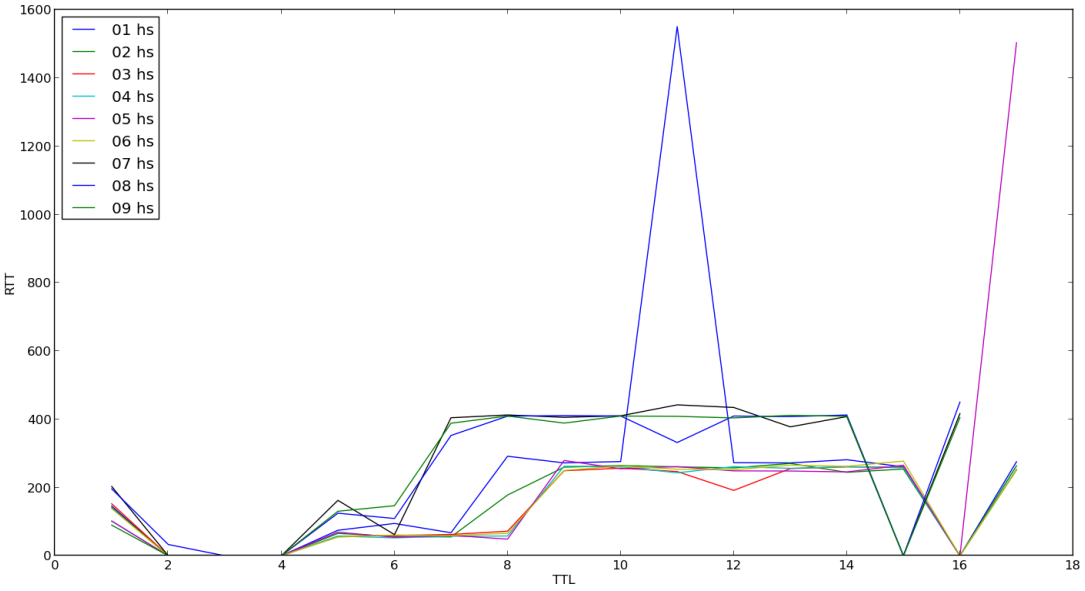

Figure 3: Canada Muestra 3

Por ejemplo, en el gráfico 2, el RTT tiene un aumento vertiginoso entre el TLL 4 y el 5, que es cuando los paquetes llegan a Estados Unidos. Sucede algo similar en 1 sólo que se da entre el TLL 7 y el 8 en algunos casos y entre el 8 y el 9 en otros. También en ambos casos según cada ejecución del traceroute coincide con el momento en que se envían paquetes a Estados Unidos. En 3 se da una situación similar entre los TLL's 6 y 7 y 8 y 9 también coincidiendo con un salto de los paquetes entre Argentina y Estados Unidos

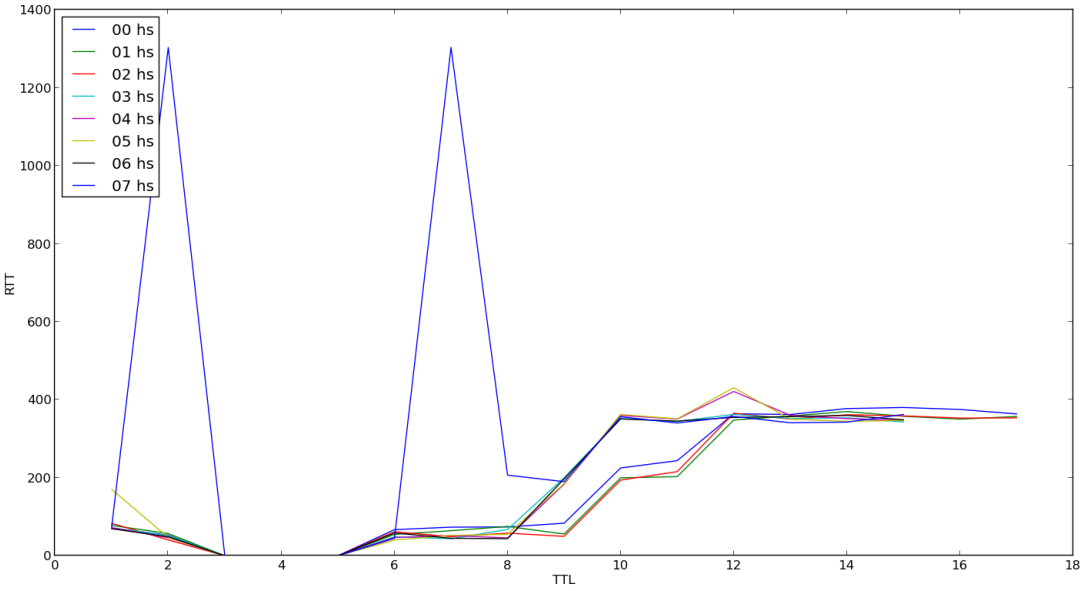

Figure 4: China Muestra 1

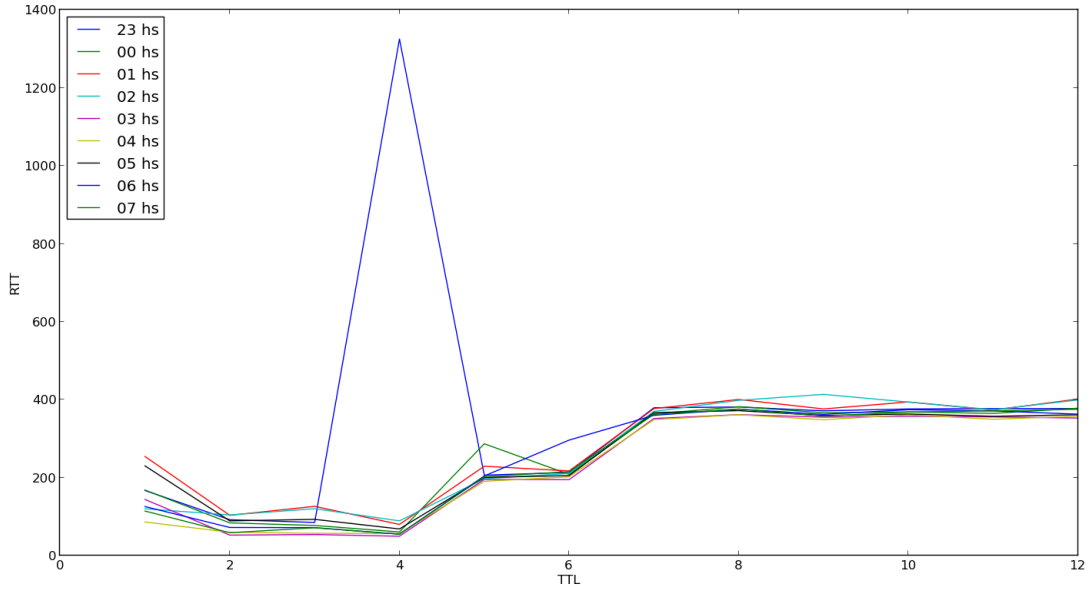

Figure 5: China Muestra 2

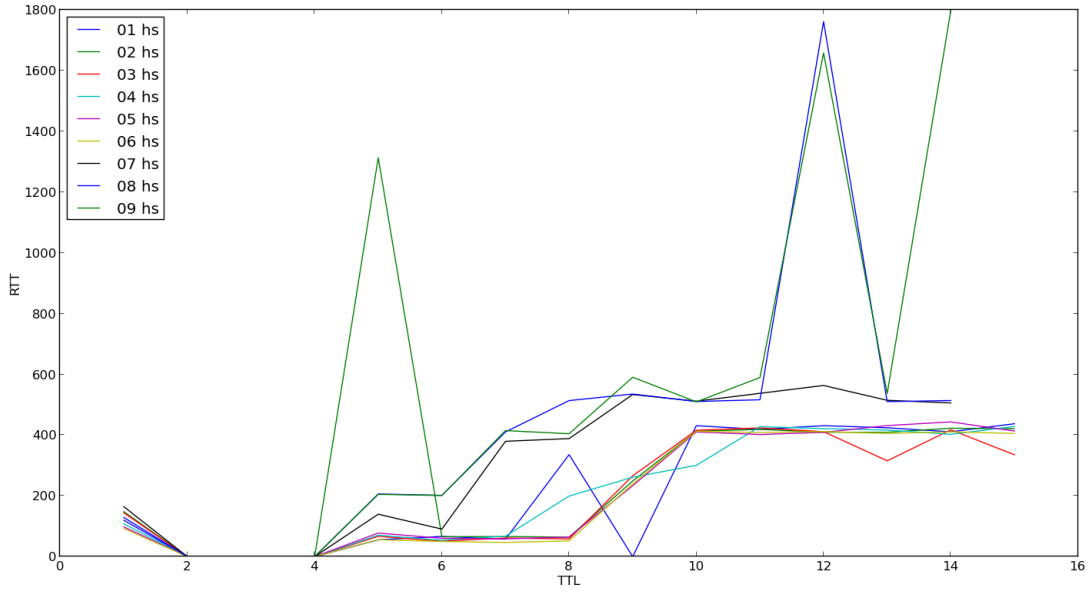

Figure 6: China Muestra 3

Con respecto a las pruebas realizadas para China, en el gráfico 5 se observan dos saltos claros entre los TLL's 4 y 5 y 6 y 7 que coinciden con dos saltos entre distintas regiones de Estados Unidos. Curiosamente, el salto entre Estados Unidos y Hong Kong no presenta un RTT mucho mayor que aquel que iba a dos regiones distintas de Estados Unidos. Se puede observar algo similar en el gráfico 4y 6 en el mismo salto (que tiene como destino una IP perteneciente a la ciudad de Miami) sólo que en estos casos es entre las TLL's 9 y 10.

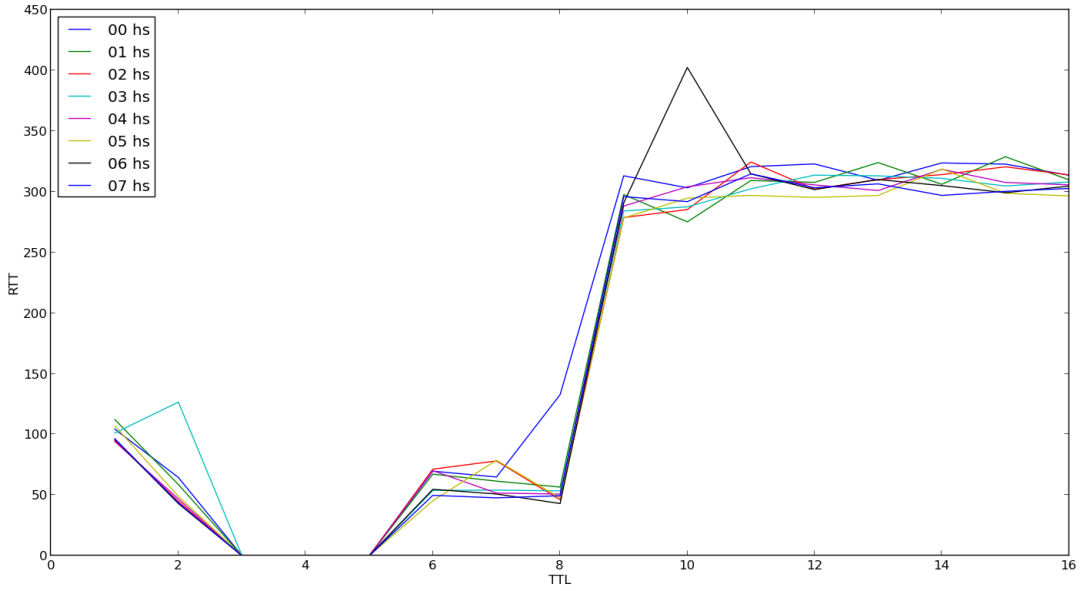

Figure 7: Rusia Muestra 1

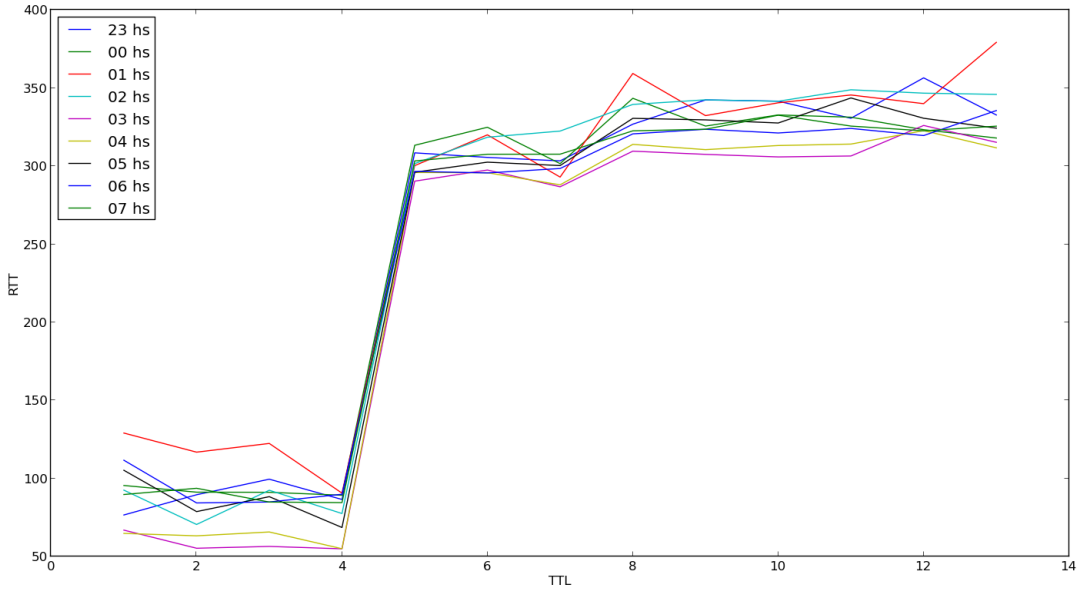

Figure 8: Rusia Muestra 2

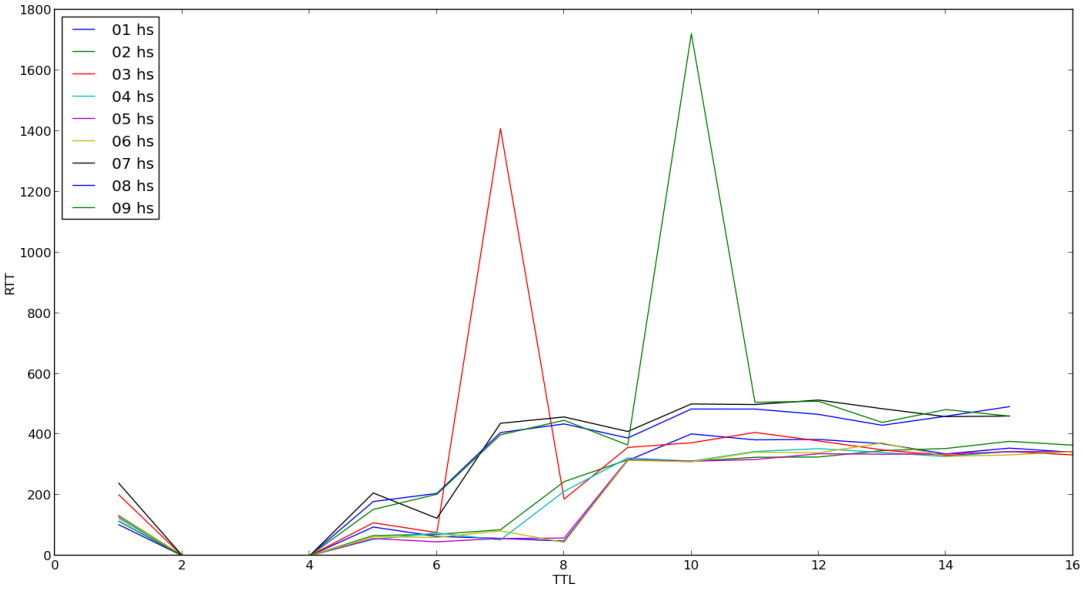

Figure 9: Rusia Muestra 3

La situación respecto a los gráficos de las pruebas realizadas para la universidad de Moscú presentan una anomalía similar a la de la universidad de Hong Kong. En todos se observa un salto más pronunciado que el resto (entre las TLL's 8 y 9 para 7, 9 y 10 para 9) y 4 y 5 para8) que coincide con dos regiones de los Estados Unidos (las mismas para todas las API's). Interpretamos que esta situación puede ser causada porque si bien la IP pertenece a las direcciones IP's de los Estados Unidos el servidor puede encontrarse en verdad en una zona geográfica más lejana.

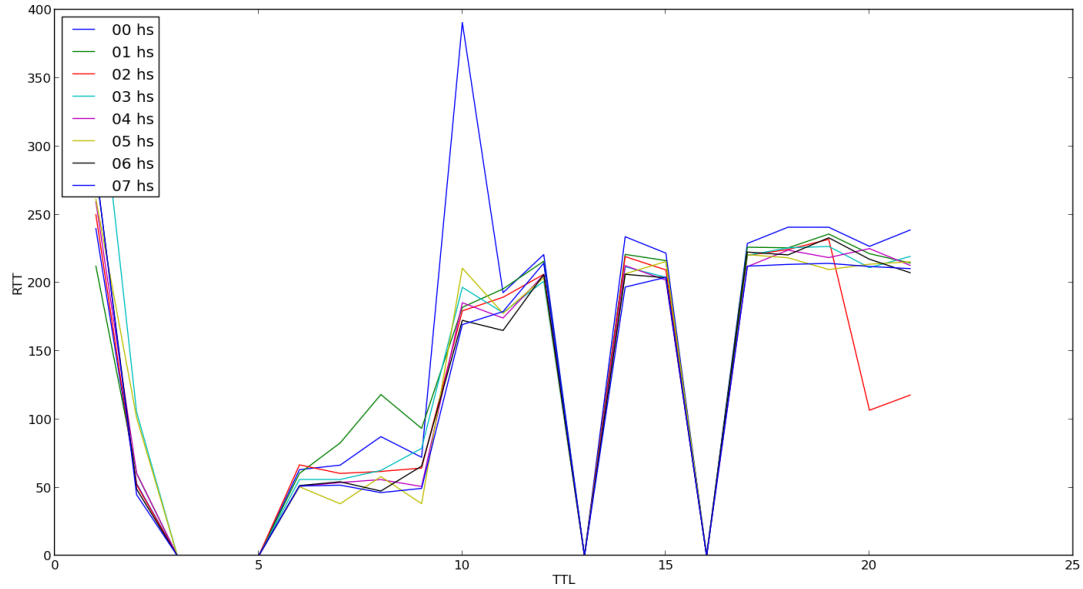

Figure 10: Samoa Muestra 1

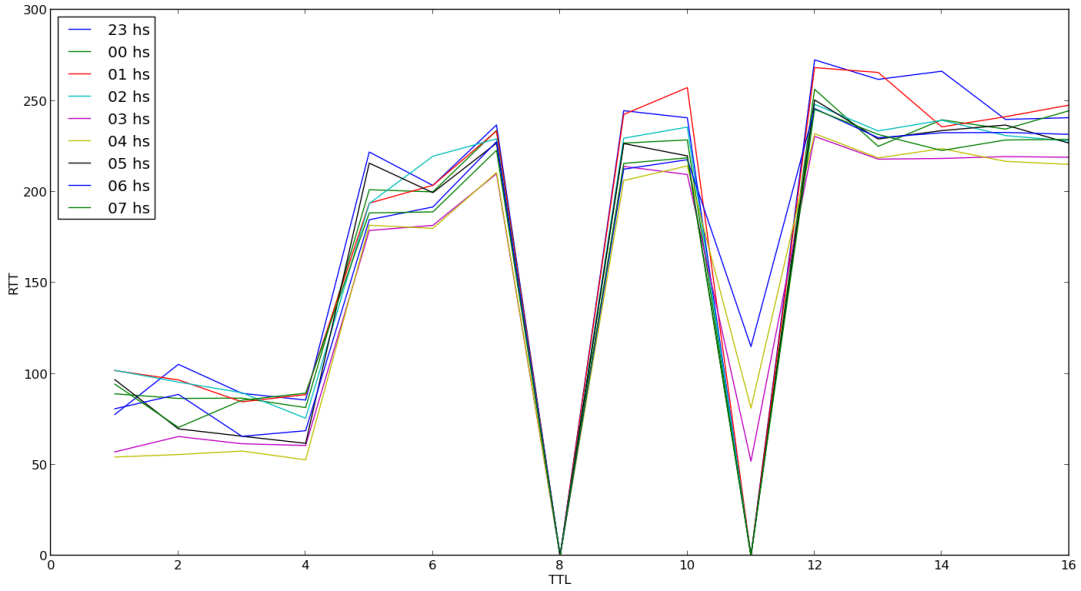

Figure 11: Samoa Muestra 2

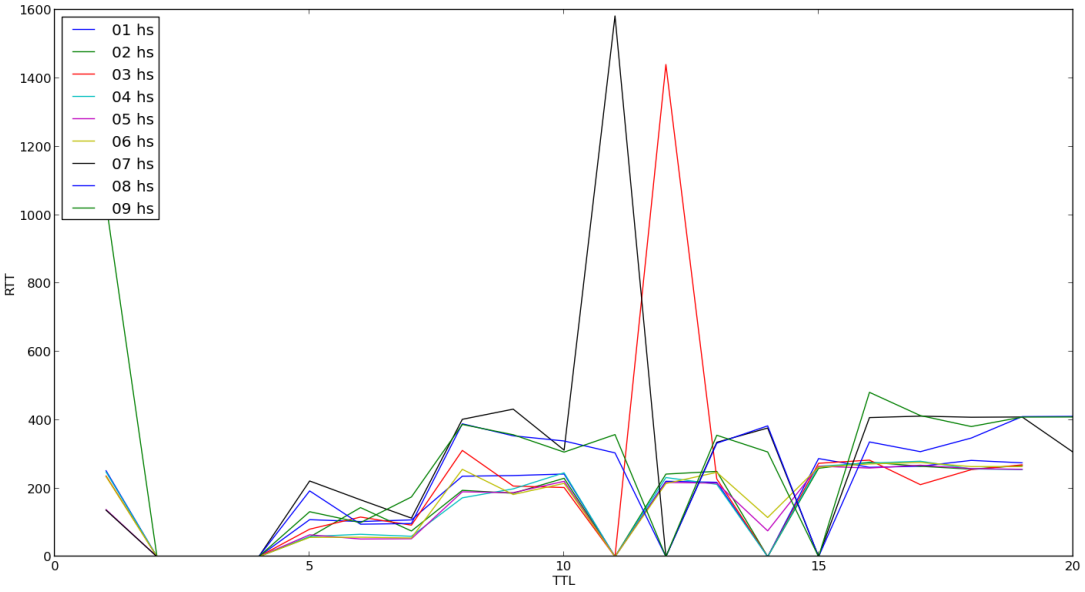

Figure 12: Samoa Muestra 3

Finalmente, en Samoa se da una situación particular: la dirección IP final del dominio de la Universidad pertenece a los Estados Unidos. Producto de una investigación y del análisis del mapa, pudimos establecer una teoría acerca de esta anomalía. A saber, que las islas pertenecientes al archipiélago en el cuál se encentra Samoa pertenecen a los Estados Unidos. Creemos que una posible explicación a este fenómeno es que Samoa no tiene ISP y utiliza los de las colonias vecinas.

Además, varios gráficos presentan picos de RTT injustificados para una hora determinada.

Este puede ser el caso de los gráficos 9 y 3, y consideramos estos picos como producto de alguna anomalía, dado que sólo ocurrieron una única vez en todas las pruebas. Por otro lado, los paquetes que no obtuvieron respuesta se pueden apreciar como un pico decreciente que llega hasta el valor 0 (que es como se representa a los paquetes que nunca retornaron). Es posible que estos paquetes no hayan tenido respuesta debido a que los routers no son compatibles con una respuesta de timeout cuando la tll llega a 0.

3.3 Segunda parte: búsqueda de enlaces transatlánticos

Los enlaces a traves de cableado submarino, también llamado enlaces transatlánticos representan un salto en cantidad respecto al **rtt**. Para lograr medir el salto en términos cualitativos calculamos el **z-score**, también denominado zrtt, con el objetivo de medir los saltos de los valores de los *rtt's* y de esta manera poder aproximar en que salto el paquete enviado atravezó un enlace submarino.

El $ZRTT$ se define de la siguiente manera:

$$ZRTT_i = \frac{RTT_i - \overline{RTT}}{SRTT} \tag{1}$$

siendo $\overline{RTT}$ y $SRTT$ el promedio y el desvío standard de los RTTs de la ruta, respectivamente, y RTT_i al RTT medido para el salto i.

Para identificar los enlaces transatlánticos es necesario encontrar un umbral que signifique un piso en cuanto al valor del $ZRTT$ que permita calificarlo como un valor distintivo. Este umbral será calculado experimentalmente sobre la base de los resultados de nuestro algoritmo de *traceroute* y con la ayuda de las herramientas de geolocalización utilizadas.

A continuación mostraremos los gráficos obtenidos para las universidades, a partir de una experimentación en la que calculamos el rtt promedio y zrtt y los comparamos en un mismo gráfico:

A nivel general, podremos observar que los mayores valores de los *zrtt's* coinciden con los saltos más grandes de los valores de los rtt's.

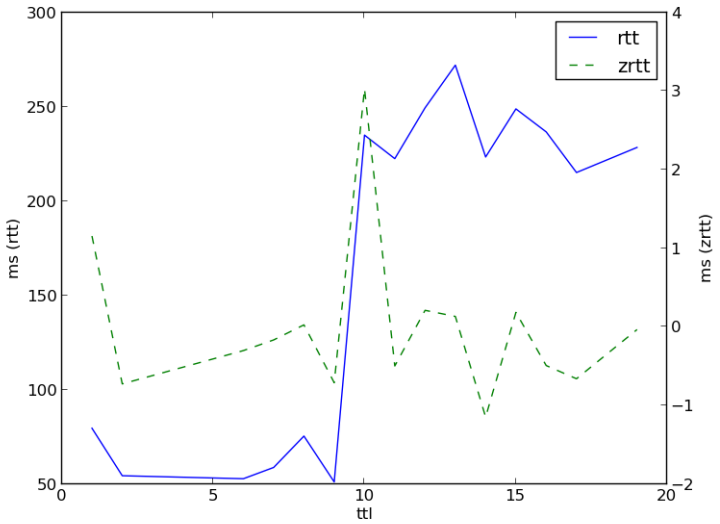

Figure 13: Canada

En el caso de Canadá, el mayor valor entre los $ZRTT's$ coincide con el salto entre una dirección IP perteneciente a la Argentina y otra perteneciente a los Estados Unidos entre el *hop* 9 y el 10.

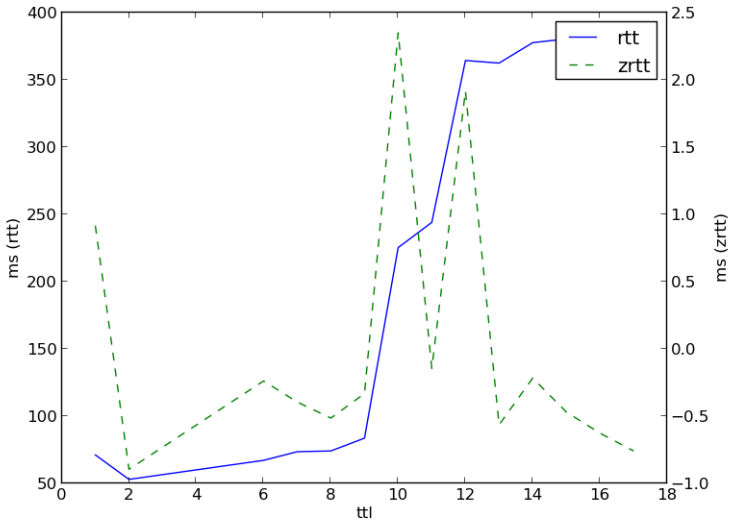

Figure 14: China

Para el caso de China, observamos que se destacan dos picos en los valores de los $ZRTT's$ para los paquetes enviados con tll's 10 y 12 los cuales coinciden perfectamente con los saltos que se producen entre una dirección IP localizada por nuestra API de geolocalización[1] en Argentina (hop 9) y otra de Estados Unidos (en el hop 10), por un lado, y entre una IP localizada en los Estados Unidos y Hong Kong por el otro entre el hop 11 y el 12. En este caso, además de identificar dos enlaces submarinos, el valor del $ZRTT$ permite comparar ambos enlaces entre sí aportando una impresión sobre la distancia y el tiempo que tarda un paquete en recorrer cada uno de estos.

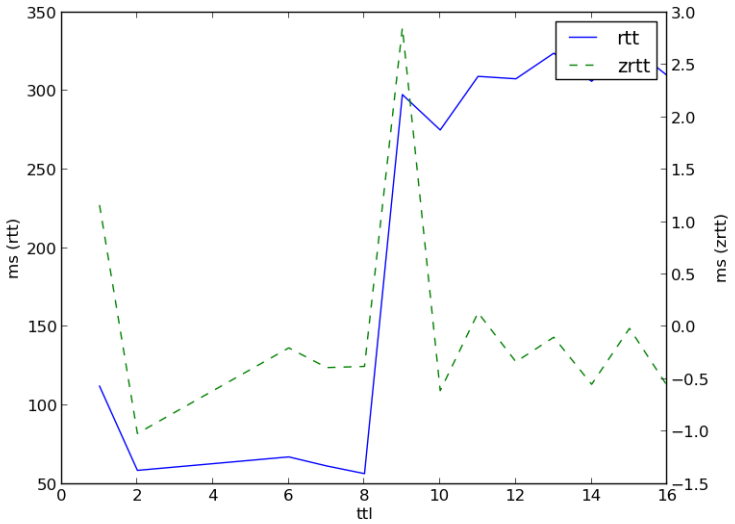

Figure 15: Rusia

En el gráfico correspondiente a los paquetes enviados a la Universidad de Moscú se observa

[1]Utilizamos tres API's distintas de geolocalización con el objetivo de complementar la información que otorga cada una y poder estimar con el mayor grado de precision las coordenadas de las direcciones IP buscadas. Las API's utilizadas son las siguientes: http://api.hostip.info; http://freegeoip.net/; y http://www.geoiptool.com/

un pico claro del valor del $ZRTT$ ubicado entre el hop 8 y el 9 que se corresponde con el enlace transatlantico que comunica una dirección IP correspondiente a la Argentina con una correspondiente a los Estados Unidos. Sin embargo, este no es el único enlace transatlántico involucrado en el envío de nuestros paquetes. Las herramientas de geolocalización dan cuenta de un salto entre direcciones IP's correspondientes a los Estados Unidos y el este de Rusia entre los hops 10 y 11. Si observamos el gráfico podemos notar que existe un pequeño aumento respecto al valor del $ZRTT$ entre esos saltos pero que es un salto mínimo que apenas logra que el $ZRTT$ tome un valor positivo apenas superior al 0. Para entender qué sucede en este caso hay que considerar que el $ZRTT$ se calcula en función del tiempo que tarda un paquete en ir y volver. Nuestro análisis explota la relación existente entre distancia y tiempo en donde, *a priori*, a mayor distancia es necesario mayor tiempo para recorrerla. Pero en la práctica es necesario considerar una multiplicidad de factores distintos que, más allá de la distancia recorrida, influyen también sobre la velocidad. A saber, esta diferencia en el tiempo que tarda un paquete en recorrer dos enlaces submarinos que conectan regiones separadas por una distancia similar puede explicarse por la calidad de la fibra del cable, por el ancho de banda de los enlaces y/o por el tráfico que hubiera en el momento de correr el algoritmo en uno y otro enlace. Recordemos simplemente que tan sólo por un tema de diferencia horaria es de esperar que los horarios de tráfico pico sean distintos. Sin embargo, a pesar de las posibles explicaciones de este fenómeno, no podemos asegurar con certeza la causa de por qué no se destaca el enlace submarino entre los Estados Unidos y la costa Este de la Federación Rusa.

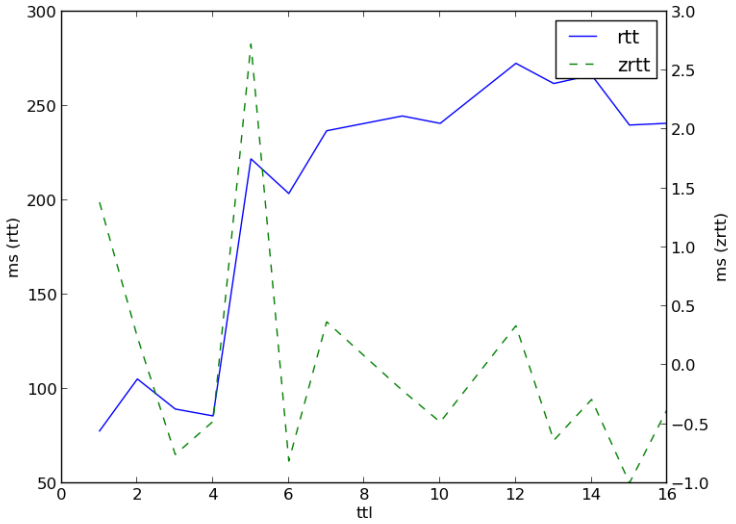

Figure 16: Samoa

Finalmente, en el gráfico correspondiente a los paquetes enviados a Samoa se observa un valor alto del $ZRTT$ entre el hop 4 y el 5 que se corresponde con el salto entre una dirección IP correspondiente a la Argentina y otra a los Estados Unidos. Podemos observar además dos saltos más de menor jerarquía en los valores de los $ZRTT's$, uno entre el hop 6 y el 7 que se corresponde con un salto entre una IP correspondiente al estado de Nueva York y otra de Washington y otro entre los hops 11 y 12 que se corresponde con un salto entre una IP correspondiente a un lugar de los Estados Unidos que no logramos identificar y otra correspondiente a Scotsdale también situado en los Estados Unidos, lugar al que también pertenece la IP de la Universidad de Samoa. Si la teoría esbozada en el apartado anterior de que la Universidad utiliza un ISP de una colonia vecina a Samoa es posible que este último salto pueda representar un nuevo enlace transatlántico. Sin embargo, debido a la diferencia de

valor que tiene con respecto al primer salto transatlántico identificado no parece ser probable que se trate de un cable submarino y estos datos, en cambio, podrían aportar a la teoría de que sensillamente la página de la Universidad de Samoa está hosteada en una compañía de hosting en los Estados Unidos.

Una observación pertinence a la hora de analizar los gráficos es que el valor del RTT del primer paquete enviado con TLL=1 suele ser considerablemente mayor que el del segundo y hasta el tercero enviados con TLL=2 y TLL=3 respectivamente. Esto genera valores muy altos del $ZRTT$ para el primer Hop. Consideramos que este fenómeno puede tener explicación en el hecho de que para todas las pruebas realizadas, el primer salto siempre se corresponde con una IP privada perteneciente, probablemente, al router de una red interna. Entendemos que este valor alto del $ZRTT$ puede tener que ver con la forma de resolver un *response* de *timeout* para un paquete que no logra salir de la propia red LAN local.

Más allá de que en todos los gráficos se observan picos en los valores de los $ZRTT's$ que permiten identificar enlaces de longitud superior (que pueden presuponerse como transatlánticos) el rango de posibles valores que puede adoptar un $ZRTT$ puede variar ostensiblemente entre el conjunto de $RTT's$ de una prueba y los de otra debido a que este rango de valores depende de propiedades que varían tal como la desviación estándar o el promedio (que pueden ser y son bastante distintos entre los resultados de una ejecución del *traceroute* y otra). Sin embargo, observando los gráficos se puede observar empíricamente que todos los hops donde se presupone un enlace transatlántico tienen un valor de $ZRTT$ superior a 1,5 (en algunos casos llegan a 2 o 2,5). A su vez, observamos que ningún otro salto tiene un valor de $ZRTT$ superior a 1. Podemos estimar un umbral que permita distinguir un hop como transatlántico sobre la base de nuestros resultados en 1,5. De esta manera, al correr nuevas pruebas, utilizando este umbral, podremos identificar los enlaces submarinos con facilidad.

3.4 Mapas

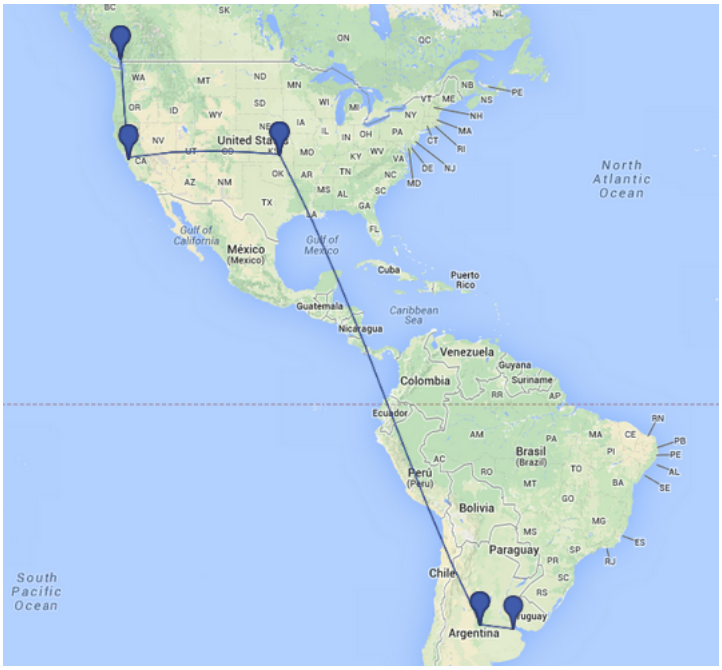

Figure 17: Canada

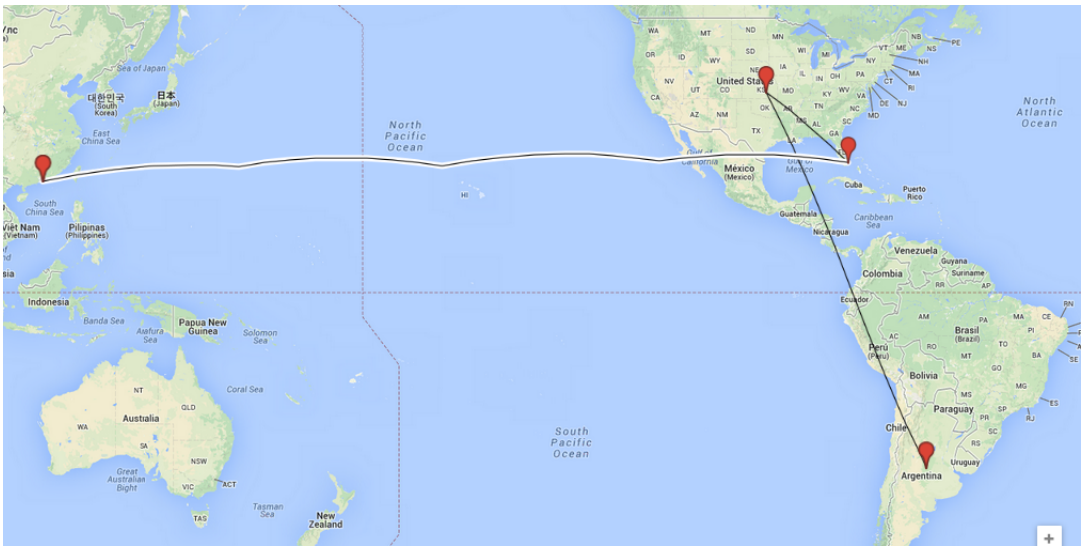

Figure 18: China

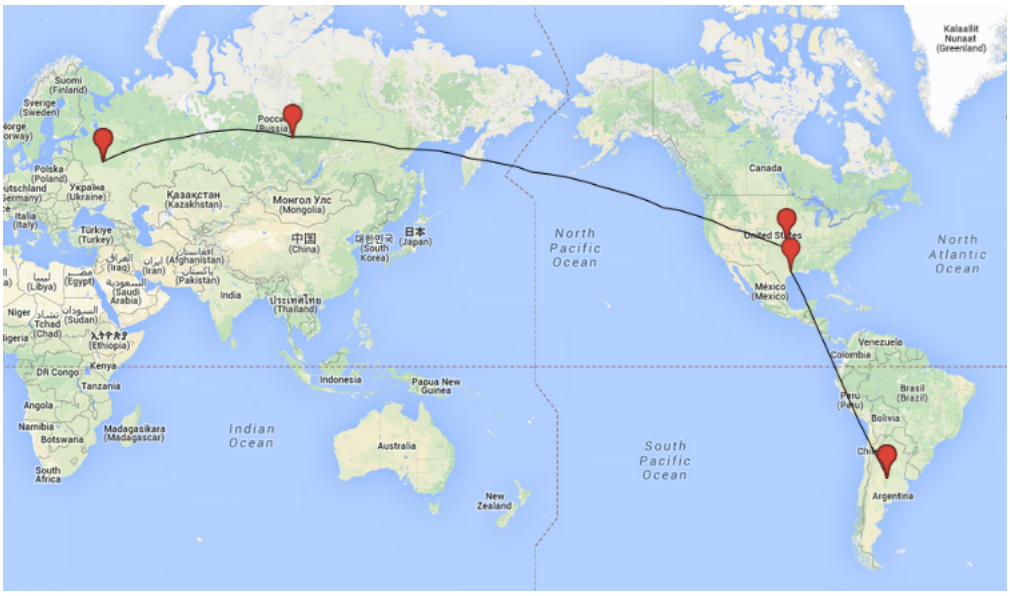

Figure 19: Rusia

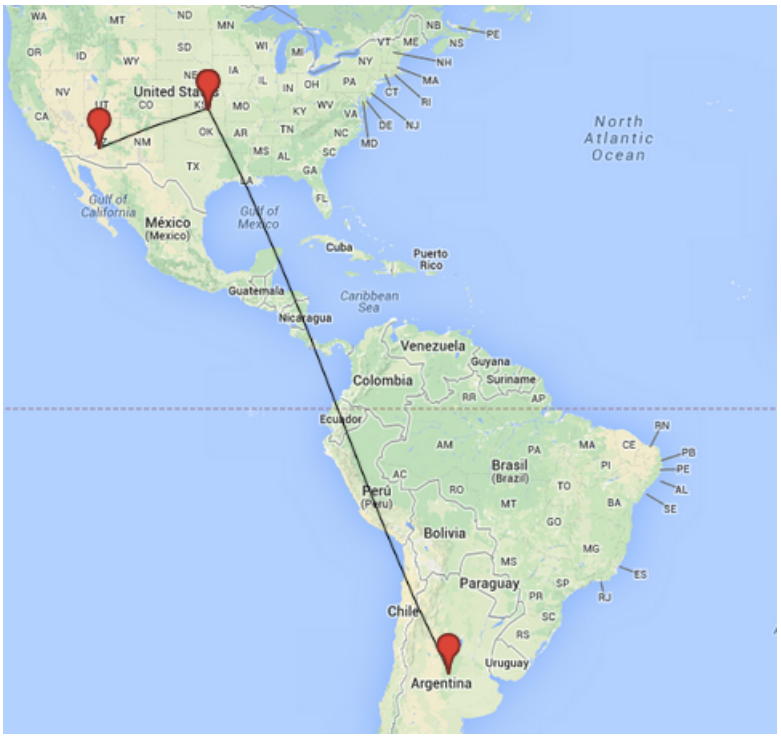

Figure 20: Samoa

4 Conclusiones

Luego de realizadas las observaciones sobre una gran cantidad de resultados, podemos corroborar, como es de esperarse, que en general los mayores tiempos se producen en los enlaces submarinos.

Pero decir esto, no es realmente pensar en lo que pudimos observar. Si bien nos aseguramos en lineas generales que eso ocurre, nos encontramos con algunos resultados que no estaban dentro de lo esperado. Sin dudas, esto se debe a la naturaleza de Internet, por ser una red tan grande y diversa, podemos encontrar grandes delays provocados por congestión, podemos encontrarnos también con nodos que no van a darnos respuestas, ya sea por ser obsoletos o por su configuración. Tambien, vimos como las rutas de los paquetes cambian, no son algo estático.

Sin embargo, pudimos notar, que aún realizando los experimentos desde dinstintos lugares, con distintos proveedores de Internet, y en distintos horarios, las rutas seguidas por los paquetes, son geográficamente similares. Esto se debe, en caso de estar enviando paquetes hacia otro continente, a que no existen muchos enlaces submarinos, sino que para poder llegar al otro lado del océano, nuestros paquetes atravesaron seguramente un mismo enlace, o conjunto de enlaces. A su vez, mediante nuestra experimentación logramos comprobar que estos enlaces no son dificiles de identificar y que puede calcularse un umbral a través del cual si el valor del $ZRTT$ de un hop es superior al enlace probablemente sea un enlace submarino.