DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Teoría de las comunicaciones

DC - UBA

Trabajo Práctico N°2

Integrante	LU	Correo electrónico
Rodrigo Kapobel	695/12	rok_35@live.com
Esteban Luciano Rey	657/10	estebanlucianorey@gmail.com
Nicolas Hernandez	122/13	nicoh22@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) 4576-3300
http://www.exactas.uba.ar

Índice

1. Introducción

1.1. Introducción

En el diseño y análisis de redes, el conocimiento de la distribución de los nodos en la red es información de suma utilidad. El comando traceroute, dada una IP, mapea el camino que los paquetes hacen desde el host que inicia el pedido hasta dicha IP, mostrando cada router que se encuentra en el camino.

No obstante, los datos no siempre son suficientes para obtener el camino deseado. En el siguiente trabajo se lleva a cabo una implementación similar a la del comando traceroute y se analizan los problemas inherentes a su funcionamiento, así como también se realiza un análisis sobre la distribución geográfica de los nodos obtenidos en una ejecución del programa.

Para nuestra implementación del algoritmo de traceroute se van a enviar y recibir paquetes de protocolo ICMP. El mismo es un protocolo de control que forma parte del nucleo de la arquitectura TCP/IP y debe ser implementado en cada nodo IP.

El header de estos paquetes posee un campo *tipo*. Vamos a enviar paquetes de tipo 8 (echo request) y esperamos recibir de los distintos nodos de la red paquetes de tipo 11 (time exceeded).

2. Diseño del traceroute

La idea general de la siguiente implementación del traceroute es la siguiente: Estando en un host, la única forma de visualizar la red es mediante el envío de mensajes. Los mensajes a enviar son paquetes ICMP del tipo *echo request* con dirección de destino a la universidad correspondiente.

Pero, con el fin de obtener respuestas de los nodos intermedios, modificamos incrementalmente (comenzando desde 1) el campo *ttl* del encabezado del paquete hasta que nos responde el nodo destino.

Entonces, cuando llega el paquete a un nodo, si su *ttl* esta en cero debería responder con un paquete de tipo *time exceeded*. Sabiendo que este es el comportamiento usual de los nodos que implementan ICMP, para cada valor posible de *ttl* medimos el tiempo que tarda un nodo en responder. A esta medición la consideramos el RTT desde el host inicial hasta el nodo.

Pero sabemos también que el medio por el cual viajan estos datos no es confiable ni libre de errores. A su vez, un paquete podría tomar distintas rutas para llegar al mismo destino. En un esfuerzo por minimizar estos errores en las mediciones, para cada *ttl* tomamos 30 mediciones, promediamos sus RTTs y elegimos como IP del nodo aquel que mas veces respondió. Con esto logramos armar finalmente nuestra estimación de la ruta que siguen los paquetes para llegar al destino

Luego, con el tiempo (RTT) obtenido de los distintos saltos, se podrá inferir si cada salto producido fue o no internacional. Para ello, vamos a trabajar sobre la hipótesis de que los saltos internacionales son los que mayor tiempo requieren en ser alcanzados, en comparación a los saltos locales (producto del distanciamiento de los routers por los enlaces continentales). Tomando las diferencias entre 2 saltos consecutivos y utilizando el método de Cimbala para detectar outliers de esas diferencias, todos los datos etiquetados como tales serán considerados saltos internacionales.

A pesar de usar muchas mediciones y promediarlas, todavía se observaban anomalías en los resultados del algoritmo. Una de ellas es que un salto más adelante en la ruta tenga menor RTT que un salto anterior. Para corregir esto tomamos el valor absoluto para la diferencia de RTT entre saltos; La idea seria que si

las diferencias son pequeñas, el haber obtenido ese resultado se pudo simplemente deber a un tema de encolamiento de paquetes a ser atendidos en el *gateway* previo. En general esto es lo que suponemos que sucede y se puede desestimar pensando que en realidad la diferencia es positiva. Para las diferencias grandes tendríamos que reconocer que nos sabemos que puede suceder, mencionando que podría darnos que un enlace es intercontinental cuando no lo es, pero mencionar que nos pareció menos agresivo que eliminar ese salto (mencionar que fue considerado como posibilidad pero desestimado al analizar las muestras para varios casos), lo cual provocaba que se inflara artificialmente la distancia entre los saltos restantes. Además, esto de los negativos sucedió bastante, por lo cual, tendríamos que haber eliminado muchos saltos.

Para los saltos que no responden mencionar que tomamos un promedio de RTTS para asignarle a estos saltos. Nuestro objetivo sería no tener que eliminar esos saltos lo cual llevaría también a un caso de inflar artificialmente la distancia entre los saltos que quedan. Aunque tampoco nos libra del todo de que esto ultimo suceda (se podrá ver en los resultados) Pero logra mitigarlo en en gran medida.

3. Experimentación

Para experimentar con el traceroute programado utilizamos los dominios de las siguientes universidades:

Universidad	Dominio
Nacional de Córdoba	www.unc.edu.ar
Stanford	www.stanford.edu
Imperial College London	www.imperial.ac.uk

Todas las muestras fueron tomadas desde General Urquiza, lo que nos permite comparar algunos resultados independientemente del origen de la muestra. Se obtuvieron todas las rutas con un ttl máximo de 30. Con 30 repeticiones para cada salto y 3 intentos en caso de no respuesta. Estos números fueron conseguidos mediante prueba y error a medida que se corría cada caso. Para geolocalizar las ips usamos realizamos una consulta GET a `http://ip-api.com/`. Dada la variabilidad con la que la página obtiene las coordenadas, los resultados al momento de la redacción del informe pueden diferir si desean constarse nuevamente.

De los resultados obtenidos con esta configuración, aún nos sorprende bastante las rutas generadas, ya que los saltos producidos entre cada gateway, en algunos casos, parecieran no tener sentido. Se verá esto en más detalle a medida que se presenten los resultados.

Cabe destacar que se intentó realizar el traceroute para la Universidad Nacional de Rosario, pero las siguientes anomalías surgieron al correr el algoritmo:

1. No finalización
2. No se obtuvo respuesta de muchos *gateways*

En ambos casos, por lo mencionado en [1, 3.1 Missing Hops y 3.2 Missing Destination] algunos routers suelen estar protegidos mediante *firewall* o configurados para no responder a ICMP time exceeded. Una razón posible para realizar estas configuraciones es que existe un ataque llamado *Smurf attack* que se define como un tipo de ataque de denegación de servicio en el cual una gran cantidad de paquetes ICMP con una IP objetivo se envían a la misma, logrando que se sature en la tarea de responder los paquetes ICMP time exceeded y por lo tanto le sea imposible responder otros pedidos.

Aunque el router no es capas de responder a paquetes ICMP, puede reenviar aquellos paquetes con $ttl > 0$ y por lo tanto el traceroute podría nunca detectar que llega a destino si no se pone un limite a la cantidad de saltos.

Aun así, para nuestro algoritmo creamos una cantidad de saltos límite de 30 $ttls$ por lo que si no se detecta el destino antes del salto 30, el algoritmo corta sin obtener respuesta del destino. En este proceso se detectaron una gran cantidad de nodos sin respuesta de tipo ICMP time exceeded. Con lo cual, al igual que con el destino, podemos asumir que todos esos gateways atravesados estaban protegidos mediante firewall.

3.1. Universidad Nacional de Córdoba

3.1.1. Posible camino seguido

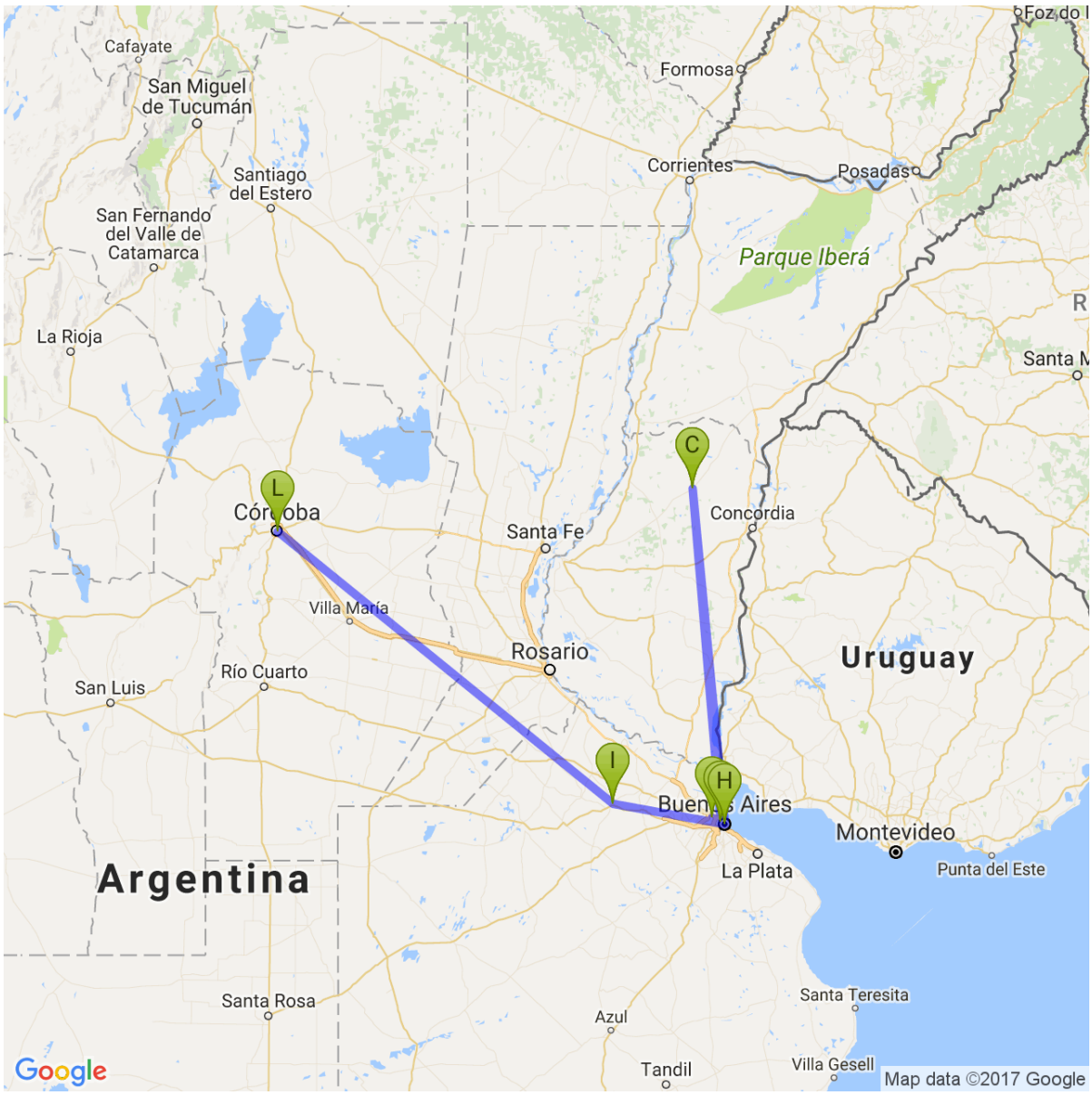

Figura 3.1: ruta de los paquetes UNC

Puede observarse que se llega a destino (marcador L). Puede observarse que la ruta no es directa, pasando por Entre Rios primero.

3.1.2. Distribución de diferencias de RTTs

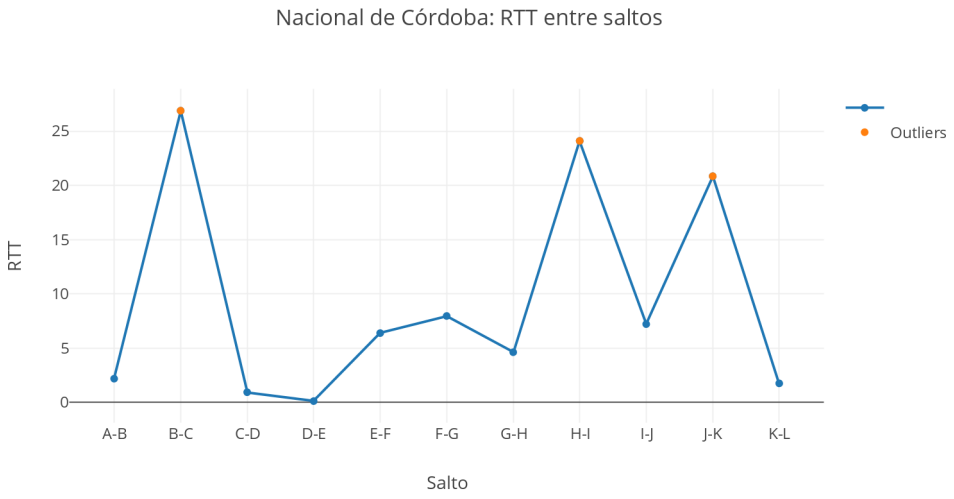

Figura 3.2: RTT entre saltos UNC

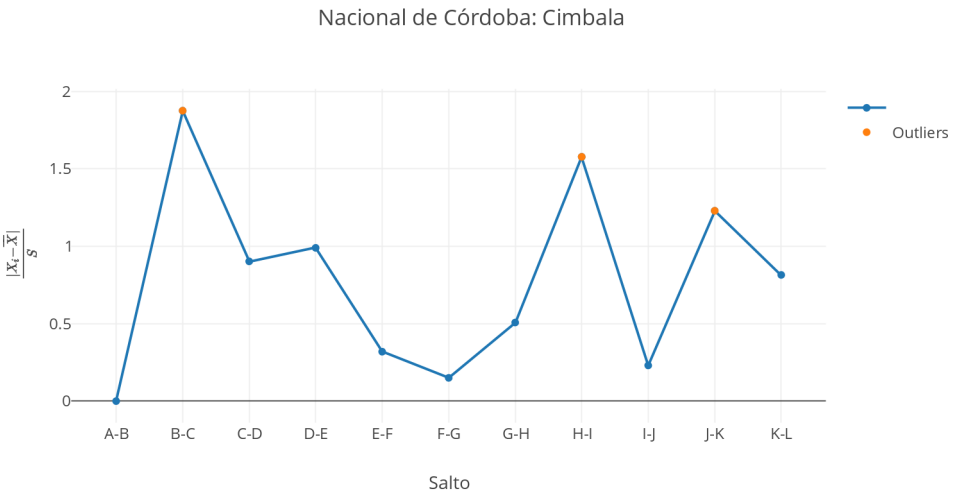

Figura 3.3: Cimbala en UNC

3.1.3. Datos derivados

El gráfico de RTT entre saltos presenta 3 picos claros:

IP	Ciudad/País	Salto
200.3.60.191	Federal Entre Rios	B-C
181.209.64.1	Carmen de Areco Buenos Aires	H-I
200.16.16.66	Córdoba Capital	J-K

Al calcular saltos intercontinentales tuvimos 3 falsos positivos que son los que pueden observarse en la tabla. Esto puede deberse a que las distancias recorridas generan rtts que no son despreciables dentro de la muestra y el algoritmo las etiqueta como outliers ya que no cuenta con la suficiente información para discernir cuando el gateway se encuentra dentro del mismo país o se ha realizado un salto internacional para llegar hasta él.

Falsos positivos	3
Falsos negativos	0

3.2. Universidad de Stanford

3.2.1. Posible camino seguido

Figura 3.4: ruta de los paquetes Stanford

Puede observarse que se llega a destino (marcador O). Vale recalcar que la página de Stanford tal parece que estar alojada en servidores de Amazon en Seattle y por eso no da como resultado Palo Alto California como hubiésemos esperado.

3.2.2. Distribución de diferencias de RTTs

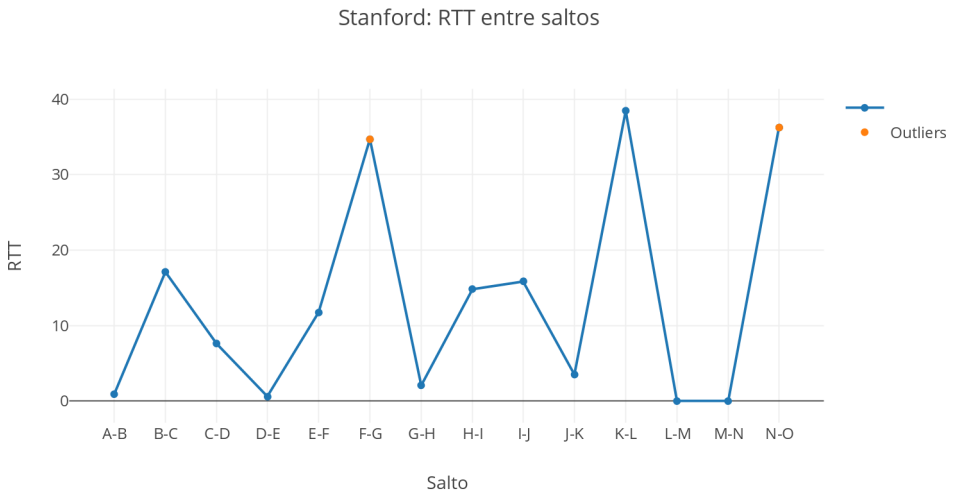

Figura 3.5: RTT entre saltos Stanford

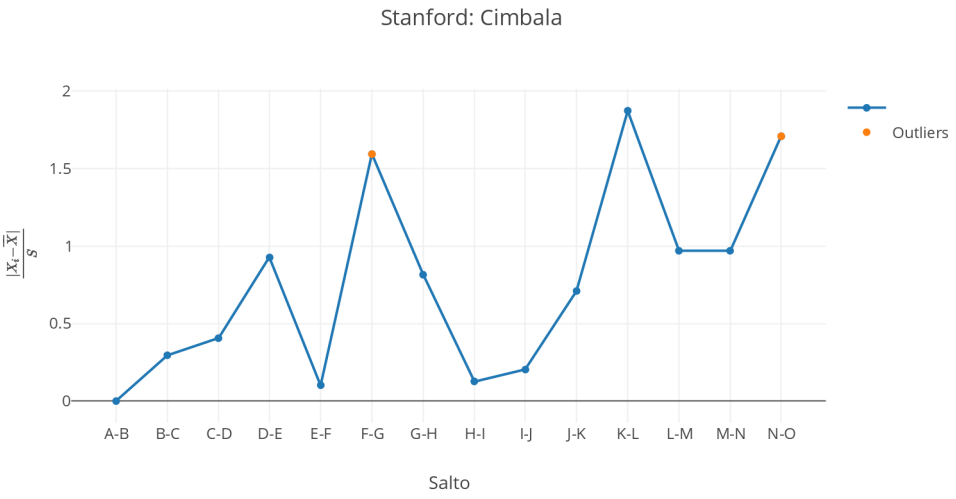

Figura 3.6: Cimbala en Stanford

3.2.3. Datos derivados

El gráfico de RTT entre saltos presenta 3 picos claros:

IP	Ciudad/País	Salto
195.22.219.31	Italia	F-G
Salto 12	indefinido	K-L
54.230.59.247	USA Washington Seattle	N-O

De los tres saltos, F-G y N-O, son aparentemente saltos internacionales ya que el algoritmo los marca como outliers. Aunque hay que aclarar que los servicios de geolocalización suelen cambiar la ubicación de las IPs haciendo difícil corroborar con certeza los resultados de cimbala.

El salto K-L se ha inflado artificialmente ya que L corresponde a un gateway sin respuesta, para los cuales se ha utilizado el promedio de RTT's en el cálculo. Aún así, el algoritmo no ha marcado este salto como internacional.

A pesar de que en el caso de (G, 195.22.219.31) la IP del salto anterior (F, 195.22.220.52) es el primer salto internacional real también a Italia, esta última no fue marcada como salto internacional. Con lo cual aquí se produce el primer falso negativo en el algoritmo para F y el primer falso positivo para G.

Se puede observar en el gráfico de Cimbala, que (I, 54.240.244.144) que corresponde a Sao Paulo Brasil no fue marcada como salto internacional a pesar de que se supone que si lo es, dado que vuelve de Italia a Brasil según la geolocalización realizada. Este último caso también se puede categorizar como un falso negativo.

En principio el destino está bien marcado como salto internacional, pero se desconoce la localización de los 3 saltos previos, por lo cual su RTT se pudo haber inflado artificialmente debido a que se utilizó el promedio como rtt para los hops previos, pudiendo dar a lugar a otro falso positivo.

Falsos positivos	1
Falsos negativos	2

3.3. Imperial College London

3.3.1. Posible camino seguido

Figura 3.7: ruta de los paquetes Imperial College London

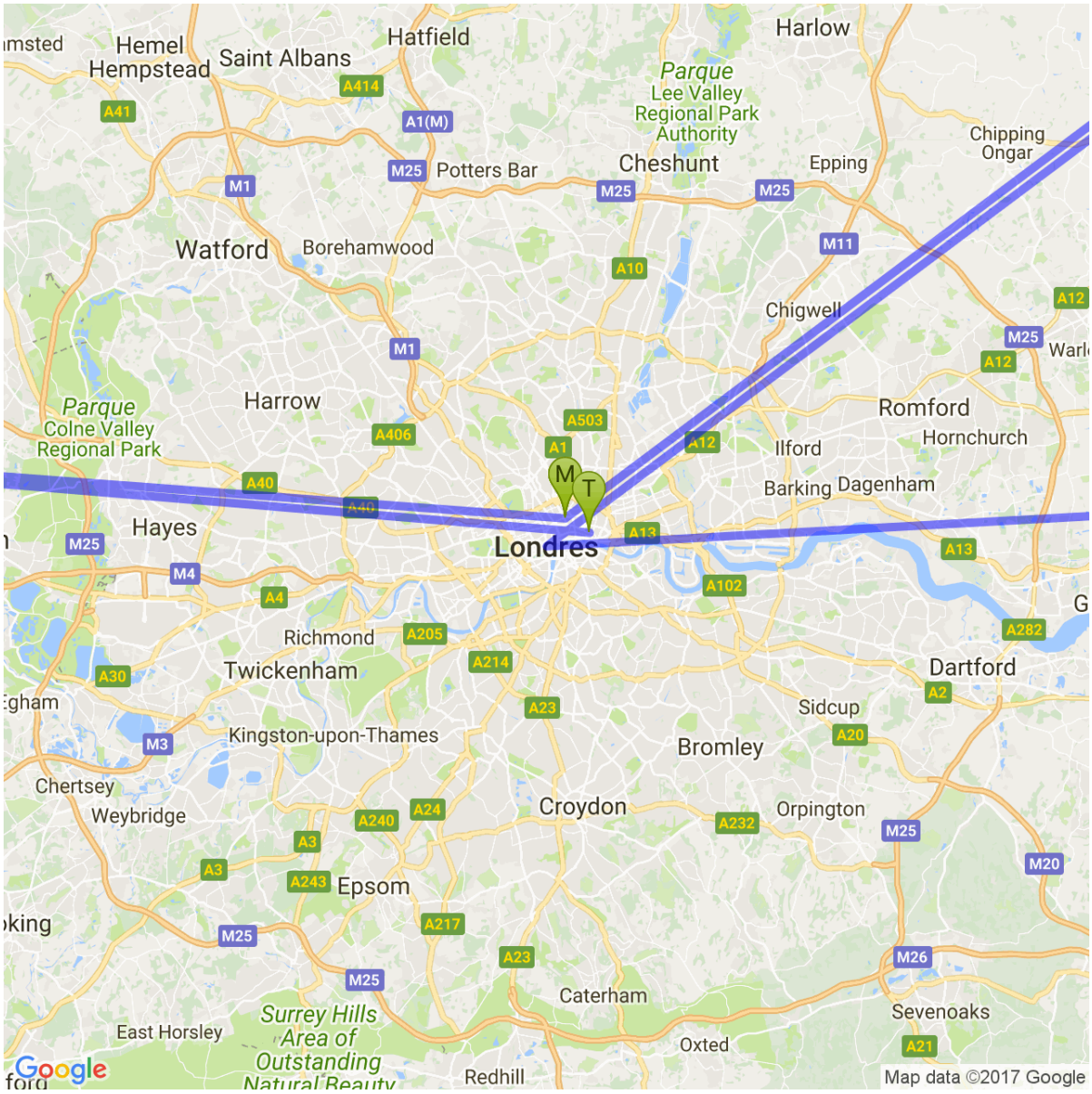

Figura 3.8: ZOOM: destino de la ruta de los paquetes Imperial College London

Se puede observar que se llega a destino correctamente (marcador T) aunque los saltos que realiza sobre todo estando cerca del destino no parecen tener mucho sentido. Dada la variabilidad de la geolocalización, sobre todo en entornos donde se necesita cada vez mayor precisión, se hace difícil un análisis cualitativo del algoritmo sin incurrir en falsos positivos o negativos.

3.3.2. Distribución de diferencias de RTTs

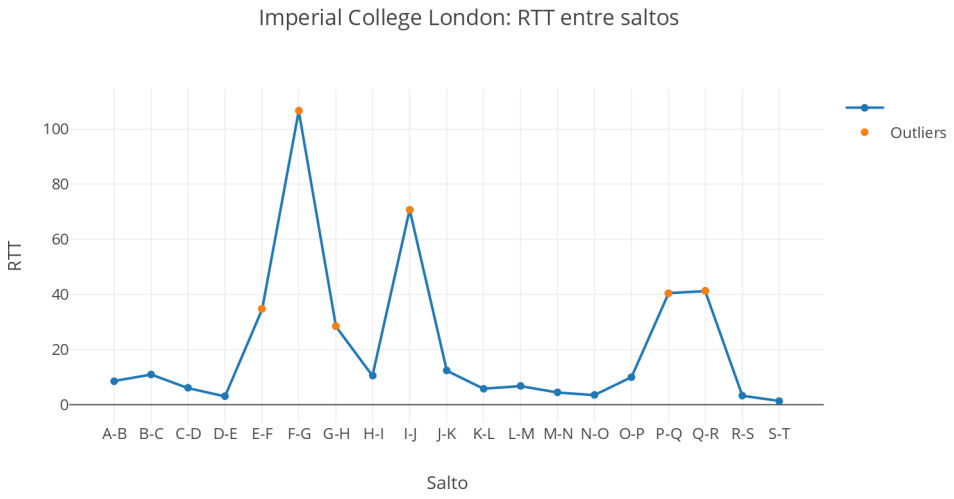

Figura 3.9: RTT entre saltos Imperial College London

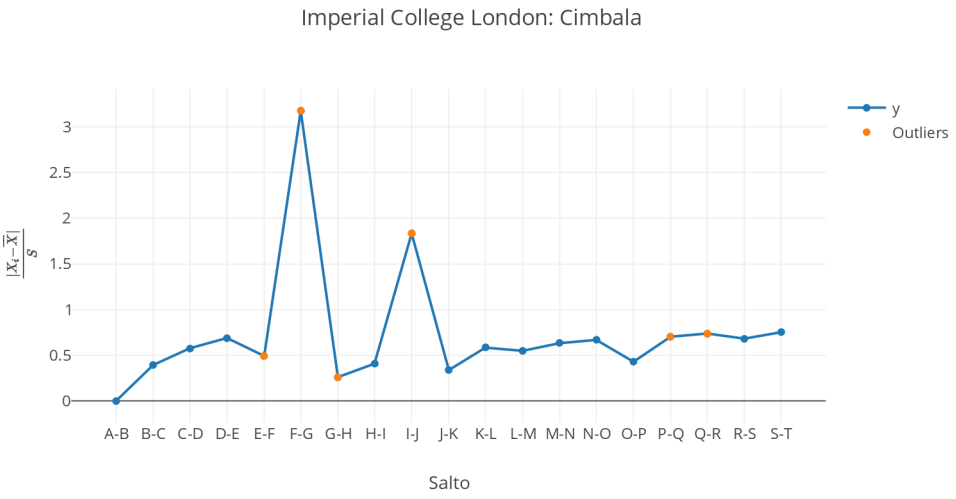

Figura 3.10: Cimbala en Imperial College London

3.3.3. Datos derivados

Los saltos que han sido etiquetados como internacionales son los siguientes:

IP	Ciudad/País	Salto
195.22.220.210	Roma Italia	E-F
89.221.41.177	Miami Florida USA	F-G
89.239.193.161	Varsovia Polonia	G-H
62.115.141.91	Londres UK	I-J
194.82.153.181	Oxford UK	P-Q
155.198.1.104	Oxford UK	Q-R

El primer salto internacional es de hecho (F, 195.22.220.210) en Roma, Italia, que es el salto previo a (G, 89.221.41.177) de Miami.

El siguiente salto a Miami es 80.239.193.161 que corresponde a Varsovia, Polonia y también fué marcado como salto internacional. Lo cual es correcto simplemente notando que son países diferentes.

En el caso de las ips de UK en principio solo la primera debería haber sido marcada como salto internacional, con lo cual aquí puede observarse dos falsos positivos.

Un falso negativo puede observarse en el salto K-L que corresponde a la ip 62.115.148.159 de Estocolmo, Suecia desde 62.115.119.145 en UK. El algoritmo no marca este salto como internacional. Un motivo podría ser que la diferencia de RTT con respecto al salto previo es menor a 20 ms con lo cual el algoritmo lo descarta como outlier. Además es un salto particular siendo que los saltos previos y siguientes se producen dentro de UK.

Falsos positivos	3
Falsos negativos	2

4. Conclusiones

Tomando en cuenta las anomalías del traceroute presentes en la bibliografia, en la sección de experimentación pudimos observar las siguientes: En el caso de la Universidad de Rosario, obtuvimos la de destino no alcanzable; explicado en la bibliografía como posible resultado de la presencia de un firewall intermedio bloqueando la comunicación.

Viendo la ruta hacia Stanford, podemos observar la presencia de saltos sin respuesta, también posiblemente causados por firewalls o routers que no responden el mensaje ICMP time exceeded.

Como fue explicado, el método utilizado para evitar que estos saltos produzcan resultados erróneos en los análisis finales, se resolvió generando un RTT promediado a partir de los RTT obtenidos al realizar el traceroute.

De forma general, en todos los experimentos se obtuvieron RTT entre saltos con valor negativo, producto de la presencia de MPLS o bien de rutas asimétricas (causadas por congestión en la red). En la implementación del algoritmo fueron solucionadas mediante la aplicación del modulo entre los tiempos de los pares de RTTs problemáticos. Esta heurística fue tomada en base al hecho de que sea por la presencia de un MPLS o un desvío por congestión, no hay manera correcta de determinar los verdaderos RTT, con lo cual se presenta como una aproximación viable el pensar los tiempos como *desordenados* y ordenarlos con el modulo.

Dado que se probaron rutas de distintas longitudes, se pudo ver que el algoritmo de Cimbala, dada su base estadística, predice de mejor forma los saltos que realmente son internacionales cuanto mayor cantidad de saltos a diferentes gateways se produjeron, teniendo como ejemplo corto la ruta hacia la universidad de

Córdoba y largo la ruta hacia la universidad de Inglaterra. Aunque la cantidad de falsos negativos o positivos también incrementa si la ruta posee saltos muy dispares como sucede con la universidad de Inglaterra.

Referencias

[1] Traceroute Anomalies, *a systematic overview of the most frequent traceroute anomalies* , Martin Erich Jobst. Department for Computer Science, Technische Universität München.