DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 2

Rutas en Internet

Teoría de las Comunicaciones
Primer Cuatrimestre de 2017

Integrante	LU	Correo electrónico
Borgna, Agustín	079/15	aborgna@dc.uba.ar
Gonzalez Benitez, Juan	324/14	gonzalezjuan.ab@gmail.com
Lancioni, Gian Franco	234/15	gianflancioni@gmail.com
Vazquez, Cristian	056/10	cristianvazquez4@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

Índice

El objetivo de este TP se centra en implementar y usar distintas técnicas y herramientas de diagnóstico a nivel capa de red, en particular las rutas de red que siguen determinados paquetes y los delays respectivos a cada nodo. Esto significa comprender los protocolos necesarios, implementar dichas técnicas, experimentar con ellas y por último estudiar los resultados en un marco analítico que nos permita extraer conclusiones de interés.

1. Introducción

1.1. ICMP Traceroute

Particularmente, estaremos haciendo uso de interacciones de control (es decir, no se intercambian datos) entre dispositivos de la red que nos permitirán armar una ruta especulativa desde un host a otro. Dichas interacciones pertenecen al *Internet Control Message Protocol (ICMP)*.

El header de dicho protocolo contiene un *tipo* y un *subtipo*. De dichos tipos nos interesan puntualmente 3 tipos de mensaje. Uno de ellos de *request* conocido como *'Echo request'* (tipo **8**) que se encarga de enviar a un destino en particular un pedido de *'ping'*, es decir que el destinatario rebote el mensaje al remitente.

Luego nos interesan dos tipos de mensaje de *response*, la primera es el *'Echo reply'* (tipo **0**) que emite el destinatario del *'Echo request'* si el paquete llegó en estado pertinente, y la segunda un *'Time exceeded'* (tipo **11**) que sucede cuando el *TTL (time to live)* del paquete IP emitido llegó a 0 camino al destinatario (el paquete lo envía cualquier nodo intermedio, en caso de que esté configurado para responder antes dichos escenarios).

Este último tipo de mensajes nos permitirá, a partir de iteraciones incrementales sobre el *TTL* en paquetes del tipo *'Echo request'*, armar una lista de IPs de destinos intermedios que respondieron *Time exceeded* antes de obtener un *'Echo reply'*. Este tipo de herramienta se conoce como un ***traceroute*** [1], aunque no necesariamente siempre se implementa mediante *ICMP* sino que existen variaciones sobre *TCP SYN*, *UDP* y, sin necesidad de usar *TTLs*, existe una opción sobre IP establecida por *RFC 1393* que permite enviar la mitad de paquetes necesarios para una implementación basada en *TTLs*.

Los paquetes generados y recibidos los manipulamos con el framework *Scapy* de *Python* que nos permite acceder a los campos de cada uno y, por ejemplo, determinar su tipo, *source*, además de poder determinar si hubo o no respuestas por parte del host intermedio.

1.2. Métodos

1.2.1. Primer ejercicio

Lo primero que necesitamos implementar es el *traceroute* mencionado. Como dijimos antes, se trata de enviar a lo sumo 30 [2] tandas (hasta que en alguna se reciba un *'echo-reply'*) de n iteraciones (usualmente con $n = 30$), donde para cada tanda se envían paquetes al destino seleccionado con un *TTL* fijo y se va incrementando entre tandas.

Las iteraciones se podrían hacer tanto por *TTL* como por *ruta entera*. Pero de esta última manera la relación entre saltos adyacentes es mucho menos independiente que de la primera. Esto tiene que ver con que pasa mucho más tiempo entre las primeras y las últimas muestras de cada salto (para 30 iteraciones en peor caso de 30 saltos es una diferencia de aproximadamente $30^2 = 900$ *requests* a 30), lo que significa resultados mas consistentes.

Entre envío y respuesta de los paquetes se mide con la diferencia entre el tiempo de emisión del paquete de *request* y el tiempo de emisión del paquete de *reply* (multiplicando por 1000 para medir de a milisegundos).

Para la ruta 'general' tomamos, por cada salto la IP con más apariciones de la tanda (de manera que no repita IPs entre saltos consecutivos, por ejemplo en el caso en que se agregue un nodo extra durante la medición) y el RTT promediado de la misma.

1.2.2. Segundo ejercicio

El segundo ejercicio consiste en implementar, sobre la base de la herramienta anterior, una nueva que permita encontrar saltos intercontinentales en la ruta trazada.

Esto se implementa buscando outliers con el método de Cimbala [3] sobre los *RTTs*. La idea es, sobre la distribución Z del muestreo [4] comparar las mediciones normalizadas $ZRTT_i$ contra valores de la tabla τ de Thompson para un α dado. Si el valor $ZRTT_i$ es menor que el valor de la tabla τ, entonces se lo asume un *outlier*.

Intuitivamente, los saltos intercontinentales son candidatos a *outlier* dado que se trata de canales con mucho delay.

[1] https://en.wikipedia.org/wiki/Traceroute

[2] Por default, se usa como máxima cantidad de saltos para una *traceroute* 30, si bien el diámetro de Internet es mucho mayor.

[3] http://www.mne.psu.edu/cimbala/me345/Lectures/Outliers.pdf

[4] https://en.wikipedia.org/wiki/Standard_score

2. Mediciones realizadas

Ahora mostraremos los datos obtenidos en todas las mediciones, considerando las herramientas obtenidas en los dos ejercicios de la primera etapa mas un conjunto de gráficos que aporten nuevos datos para poder analizar.

2.1. Victoria University of Wellington

Medimos a continuación la ruta a los servidores de la Universidad Victoria en Wellington, Nueva Zelanda. El host de destino elegido fue *'victoria.ac.nz'*.

Realizamos mediciones con 30 iteraciones por TTL y observamos los resultados de la figura 1.

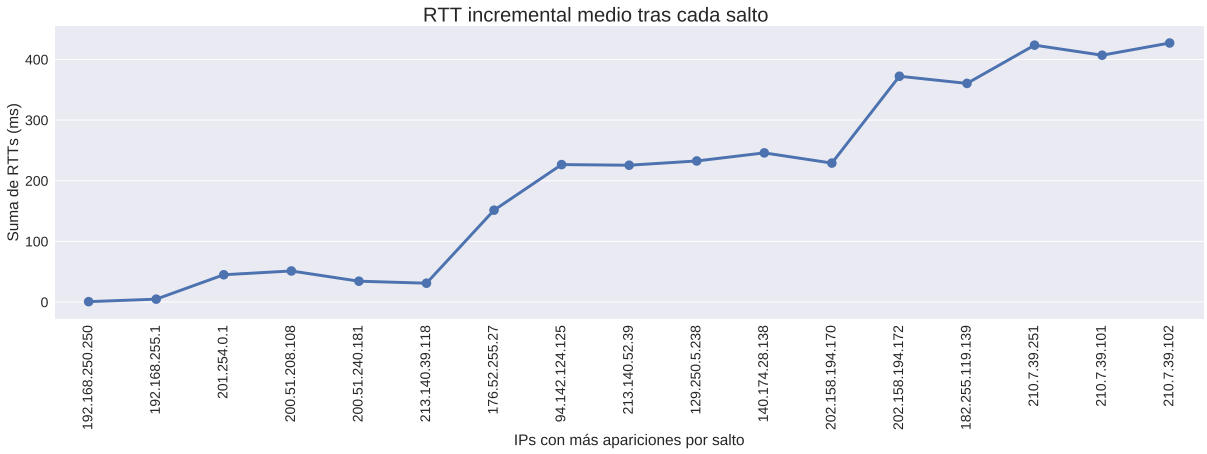

Figura 1: Comportamiento incremental de RTTs medios medidos.

Notamos tres segmentos distinguidos donde el delay se mantiene relativamente constante.

Hasta la ip 200,51,208,181 la ruta se encuentra dentro de argentina. Desde el host 213,140,39,118 hasta el 213,140,52,39 nos encontramos con ips que parecen ubicarse en España. Y luego el siguiente host tiene ip estadounidense. Este comportamiento lo observamos en todas las mediciones realizadas desde la misma red, que utiliza como isp *Speedy*, parte de Telefónica España, por lo que suponemos que los servidores en la ruta de Argentina a Estados Unidos utilizan ips de Telefónica aunque no estén ubicados en España.

Luego de pasar por Estados Unidos nos encontramos con dos ips australianas, 202,158,194,170 y 202,158,194,172, entre las cuales se produce el siguiente salto notable. Debido a la similitud entre ips suponemos que la primera se encuentra realmente en Estados Unidos y se trata de los dos extremos de un cable submarino entre este país y Australia.

Otro salto un poco mas pequeño se produce entre 182,255,119,139 y 210,7,39,251 cuando se cambia entre ips australianas y neo zelandesas, por lo que suponemos que se trata de otro cable submarino mas corto.

En la figura 2 se aprecian mas directamente estos tres saltos Argentina - Estados Unidos - Australia - Nueva Zelanda.

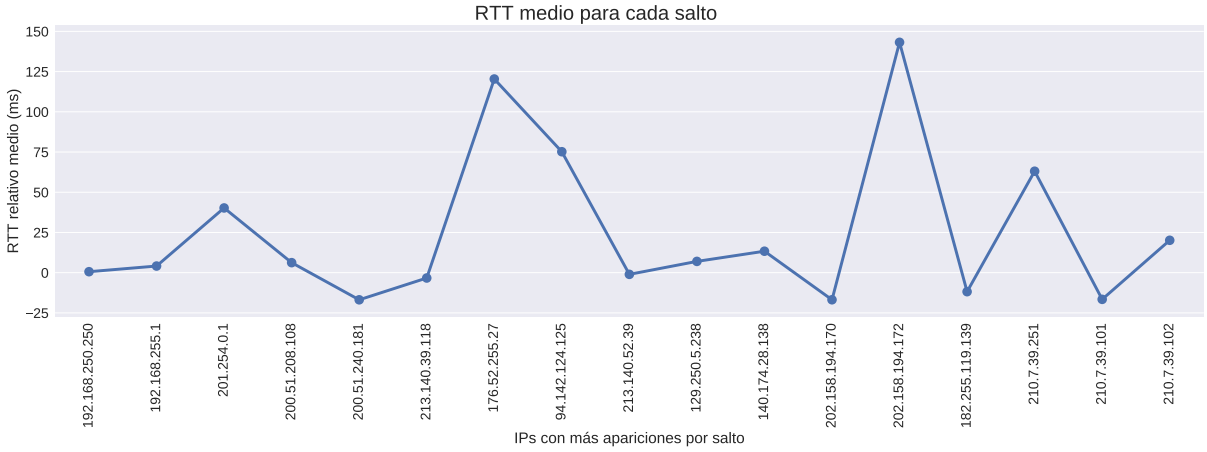

Figura 2: RTTs medios medidos para una traceroute a la Universidad Victoria de Wellington.

Vemos en el mapa de la figura 3 los tramos que nombramos, incluidas las ips españolas, distinguiendo en rojo los que presentaron mayor delay. Debido a que los sectores con mas delay de la ruta se presentaron entre ips del mismo país sólo se marca el cable Australia - Nueva Zelanda.

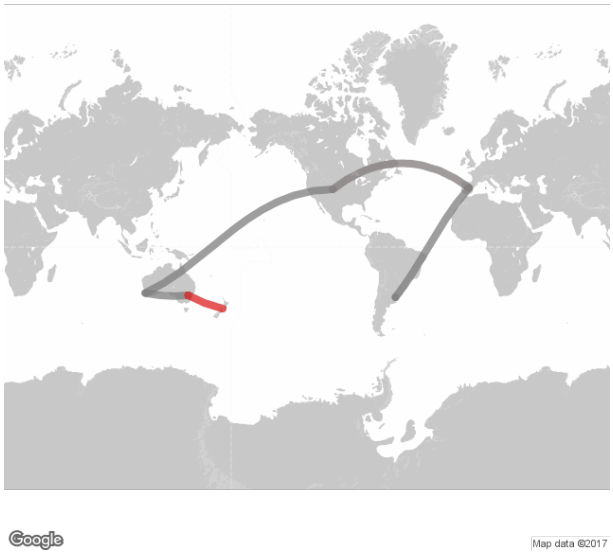

Figura 3: Mapa de ubicaciones inferidas para una traceroute a la Universidad Victoria de Wellington. Tramos con mas delay marcados en rojo.

En total, 17 de los 19 nodos de la ruta respondieron (un **89.5** %).

A continuación intentamos detectar los cables submarinos utilizando el método de Cimbala como se detalló en la sección 2.2.

Los resultados se pueden apreciar en la figura 4. Con el umbral de la tabla γ detectamos correctamente el cable entre Argentina y Estados Unidos y entre este y Australia. El tercer cable, de Australia a Nueva Zelanda, no resulta distinguido debido a su poca extensión.

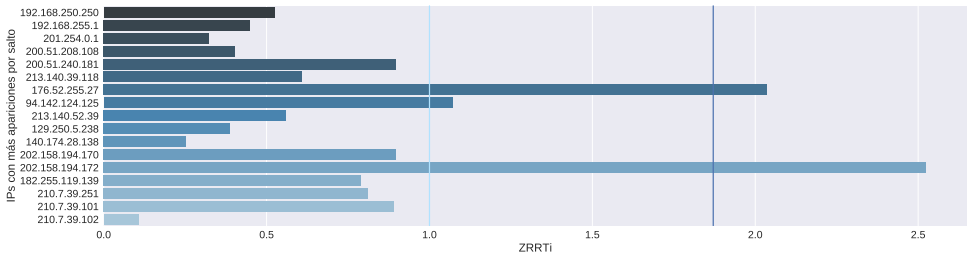

Figura 4: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

2.2. University of London

Para esta medición se eligió la Universidad de Londres (King's College, the London School of Economics and Political Science, etc), ubicada en Londres, Inglaterra. El destino propiamente dicho es *'london.ac.uk'*. Se esperaría encontrar dos tramos transatlánticos: Argentina-Miami y uno transatlántico, asumiendo paso intermedio por EEUU. Hicimos las mediciones varias veces en días aledaños y los resultados fueron siempre consistentes. Midiendo de a 30 iteraciones por TTL observamos los siguientes RTTs:

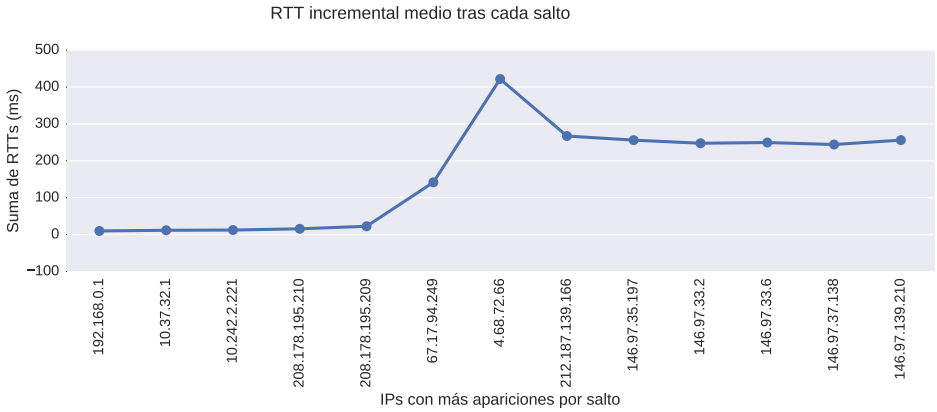

Figura 5: Comportamiento incremental de RTTs medios medidos.

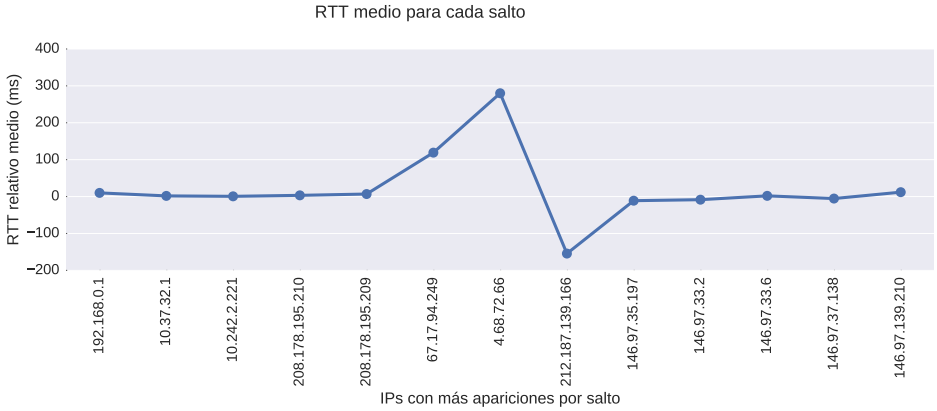

Figura 6: RTTs medios medidos para una traceroute a la Universidad de Londres.

En la figura 5 se notan dos tramos donde las diferencias entre RTTs relativos son bajas y constantes, que seguramente se corresponden al entramado interno de Buenos Aires y Londres en contraste con las

rutas submarinas con mayores promedios.

En la figura 6 se puede observar un gateway que conforma un pico, adjudicado a las IP '4.68.72.66' geolocalizada en Estados Unidos con hostname *'lag-9.ear1.Miami1.Level3.net'*. Podemos suponer que se trata de un gateway extremadamente cargado, posiblemente por estar en una red troncal respecto a enlaces submarinos. Este es el único nodo que cambió entre mediciones, dado que en las repeticiones posteriores y anteriores no era común su aparición, que quizás se deba a algún rebalanceo.

Anteriores a este salto aparecen dos nodos interesantes que son el '208.178.195.209' y '67.17.94.249', ambos adjudicados a Estados Unidos. La '208.178.195.209' destaca porque, al igual que '208.178.195.210' tiene una latencia sospechosamente similar a las locales de Argentina. Mientras que la '67.17.94.249' presenta un gran salto respecto de su anterior en términos de RTT.

Por lo cual se especula que '208.178.195.210' y '208.178.195.209' son gateways locales, partes del backbone argentino que conecta con links internacionales. Lo cual se condice con el hostname de la última: *'global-crossing-argentina-s-a.xe-0-1-0.ar3.eze1.gblx.net'*.

Esto significaría que '67.17.94.249' es el gateway del lado estadounidense del link intercontinental.

El nodo '212.187.139.166' es el primero adjudicado a Londres, siendo candidato a extremo británico del enlace transatlántico. Tiene promedio negativo, esto no sorprende, dado que su antecesor ('4.68.72.66') tenía un promedio muy alto.

Figura 7: Mapa de ubicaciones inferidas para una traceroute a la Universidad de Londres.

Se puede notar el enlace transatlántico mencionado antes, y en rojo fuerte el gateway sobrecargado de Estados Unidos.

El traceroute presenta algo curioso, y es que todos los nodos locales a Argentina tienen asignadas IPs reservadas/privadas (192.168.0.1, 10.37.32.1, 10.242.2.221). Por lo tanto el geolocalizador solamente puede empezar a reconocer nodos a partir de las IPs estadounidenses (que, como dijimos anteriormente, las primeras están mal adjudicadas dado que probablemente estén ubicadas en el extremo argentino del enlace Argentina-Miami) significando que en el mapa el punto de origen se encuentra en dicho país.

Respecto al porcentaje de nodos que respondieron los *requests* sucede otra anomalía: el host destino parecería no estar configurado para emitir respuestas de este tipo. Esto implica que el traceroute sigue emitiendo hasta llegar al límite preestablecido de los 30 *hoops*, y no poder determinar con total seguridad en qué salto se llega al destino (y cuántos en el medio no respondieron).

Asumiendo que es el último en responder (responde por *time-exceeded*, no *echo-reply*), el porcentaje sería aproximadamente del **93 %** con un único nodo mudo ubicado entre '67.17.94.249' y '4.68.72.66', es decir en el backbone estadounidense.

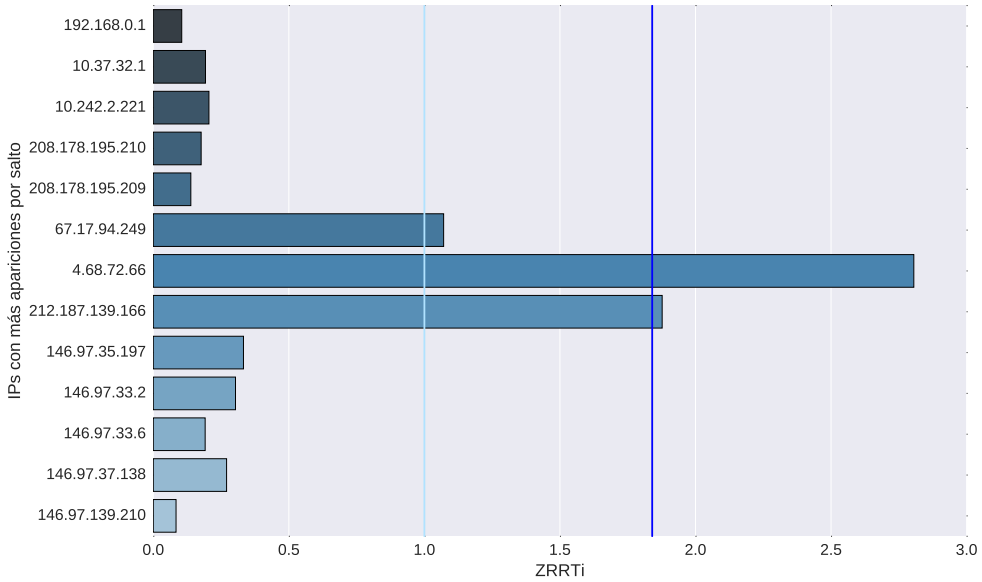

Figura 8: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

En la figura 8 se ven los outliers de la muestra. Respecto del umbral de la tabla τ, se distinguen los nodos del extremo británico del transatlántico y el gateway sobrecargado de EEUU, que no es extremo intercontinental pero sí presentó muchísima latencia.

El otro extremo intercontinental que falta, el de Argentina-Miami aparece con el umbral $Z = 1$ (es decir aquellos que están por encima de la desviación estándar normalizada) junto a los dos anteriores, pasando de un falso negativo y un falso positivo, a un único error del tipo falso positivo para el nodo en sobrecarga. Por lo tanto el modelado de la distribución es relativamente exitoso para encontrar dichos tramos, aunque el gateway más destacado no sea un tramo intercontinental.

2.3. University of Uzbekistan

Para esta medición se eligió la Universidad Nacional de Uzbekistan (O'zbekiston Milliy Universiteti), ubicada en Tashkent, Uzbekistan. El *host* correspondiente a esta universidad es *nuu.uz*.

Para esta medición se espera que la ruta se divida en tres tramos siendo el primer tramo el correspondiente a Argentina-EEUU, cruzando el Océano Atlántico hasta desembocar en Europa y finalmente desde Europa hacia el Oeste de Asia alcanzando finalmente Uzbekistan.

Las mediciones fueron realizadas en repetidas ocasiones con el objetivo de no caer en conclusiones precipitadas, utilizando en cada oportunidad 30 iteraciones por TTL. Finalmente los RTTs conseguidos fueron los siguientes:

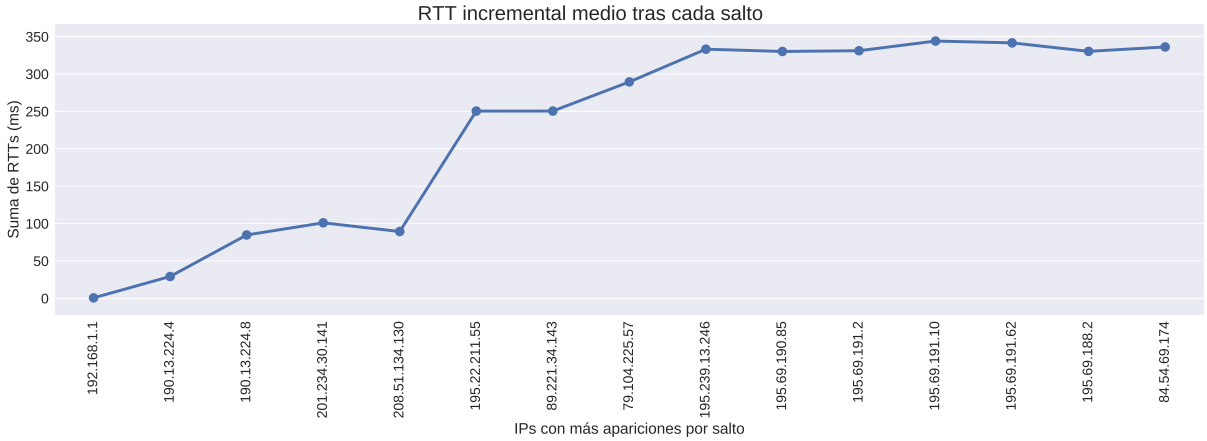

Figura 9: Comportamiento incremental de RTTs medios medidos.

En el gráfico se pueden observar dos incrementos notorios en el RTT, el primer incremento se corresponde con el tramo transatlántico que une EEUU con Europa, debido a que este es el tramo más largo.

A continuación se nota otro incremento aunque no tan notorio en el RTT seguido de un incremento más paulatino, casi constante. Este pequeño incremento nos predispone a considerar la existencia de un cuarto tramo y reconsiderar la idea inicial en la que el ultimo tramo es desde un único país Europeo hasta Uzbekistan.

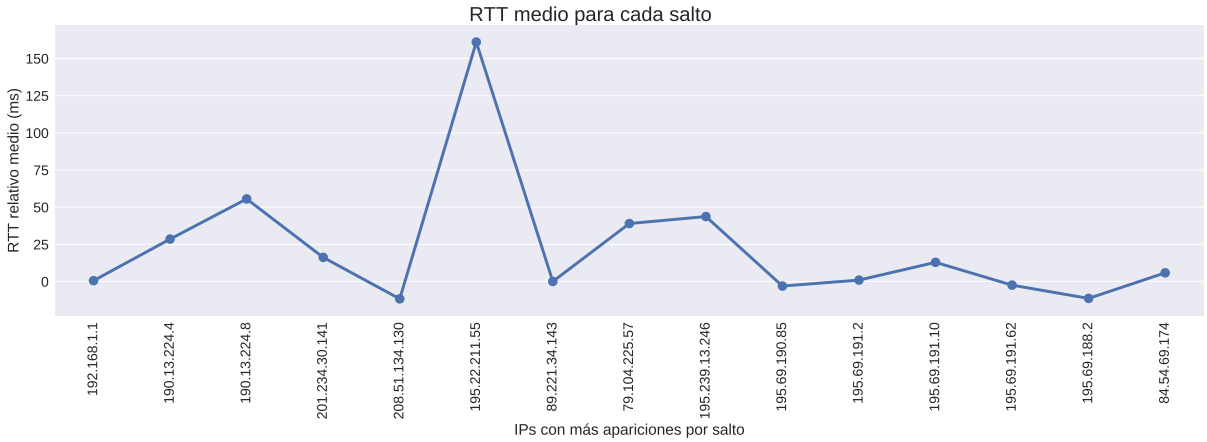

Figura 10: RTTs medios medidos para una traceroute a la Universidad de Uzbekistan.

Buscando información de la IP ’195.22.211.55’ pudimos observar que se trata de un host ubicado en Roma, Italia. Debido al incremento en el RTT medio medido para esta IP, creemos que éste es país europeo en el cual desemboca el tramo transatlántico antes de seguir rumbo hacia su destino.

Por otro lado, el incremento presente en ’195.239.13.246’, se corresponde con un host ubicado en Moscú, Rusia y es el que funciona como enlace entre Europa y Asia dándonos de este modo el cuarto tramo del recorrido.

Figura 11: Mapa de ubicaciones inferidas para una traceroute a la Universidad de Uzbekistan.

Finalmente, graficando la ruta obtenida podemos constatar que efectivamente el recorrido consta de cuatro tramos, siendo los tramos EEUU-Italia el tramo con más RTT seguido del tramo Italia-Rusia y los responsables de los picos observados en los gráficos anteriores. Considerando este gráfico podemos concluir que exite un total de 3 saltos intercontinentales (América-Europa-Asia) a pesar del tramo que une a Italia con Moscú que si bien se trata de un tramo con un RTT considerable no es un tramo intercontinental.

En esta medición asi como en las anteriores, se puede ver la misma anomalía en la que se utiliza la totalidad de los 30 *Hoops* sin poder determinar con seguridad en qué salto se llega al host destino. Teniendo esto en cuenta y que la cantidad de nodos que responden al *time-exceeded* es 15, se puede concluir que solo el 50 % de los nodos respondió al *echo-request* si contamos esta vez contra los 30 saltos máximo totales (la otra opción sería contar el último salto que responde *time-exceeded* como el destino, aunque no se pueda determinar si realmente lo es, como hicimos antes).

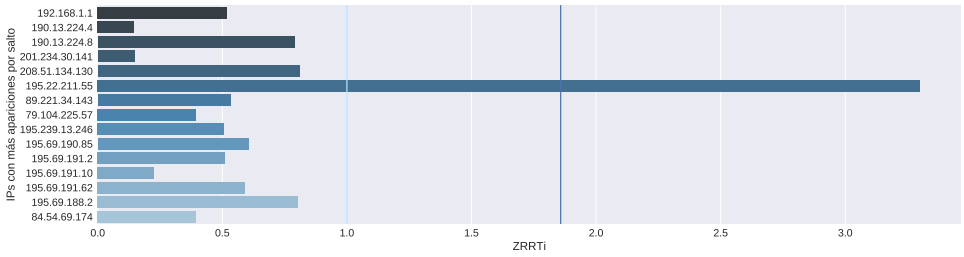

Figura 12: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

En la figura 12 se ven los outliers de la muestra. Respecto del umbral de la tabla τ. Se distingue un solo outlier correspondiente al nodo ubicado en Italia. Esto resultado es esperado debido a que se trata del extremo Europeo del tramo transatlántico alcanzando de este modo el RTT máximo de la medición sobrepasando incluso a los demás tramos intercontinentales y etiquetando a éstos últimos como falsos negativos.

2.4. Makerere University

Como siguiente caso de estudio se eligió la Universidad Makerere de Uganda, alojada en *mak.ac.ug*. Las mediciones fueron realizadas en varias oportunidades utilizando 30 iteraciones por TTL para garantizar la confiabilidad de los datos.

En la figura 13 se aprecian las mediciones de las RTTs.

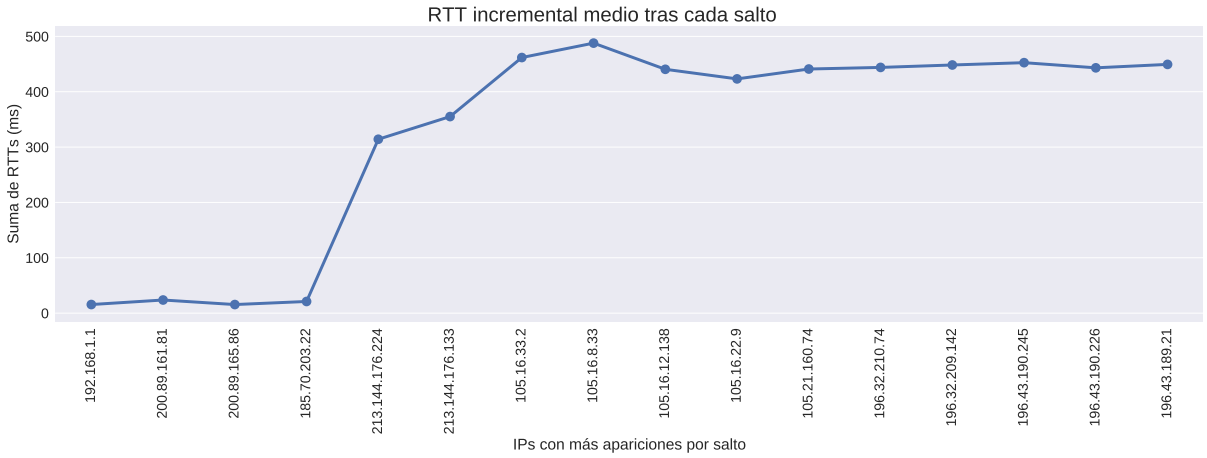

Figura 13: Comportamiento incremental de RTTs medios medidos.

Nos encontramos primero con un segmento con delay que pareciera corresponder a servidores locales, aunque vemos que la última ip $(185{,}70{,}203{,}22)$ se geolocaliza en Italia. La siguiente ip $(213{,}144{,}176{,}244)$ corresponde también a coordenadas italianas, por lo que suponemos que se trata de los dos extremos de un cable submarino.

El siguiente salto se produce en la ip $105{,}16{,}33{,}2$, que parece ahora ubicarse en Francia. Las siguientes dos ips nos llevan a la isla de Mauricio, pero no se corresponde con una diferencia notable en RTTs. Esto sumado a la similitud de estas ips con la francesa nos mueve a pensar que se trata de un cable submarino desde Italia a Mauricio, y que la ip francesa aparece por alguna razón interna de la empresa correspondiente.

Luego tenemos una sucesión de ips de Tanzania, Sudáfrica y finalmente Uganda, con poca diferencia de RTTs por lo que suponemos que se trata del enlace terrestre final.

En la figura 14 vemos mas directamente estas diferencias de RTT.

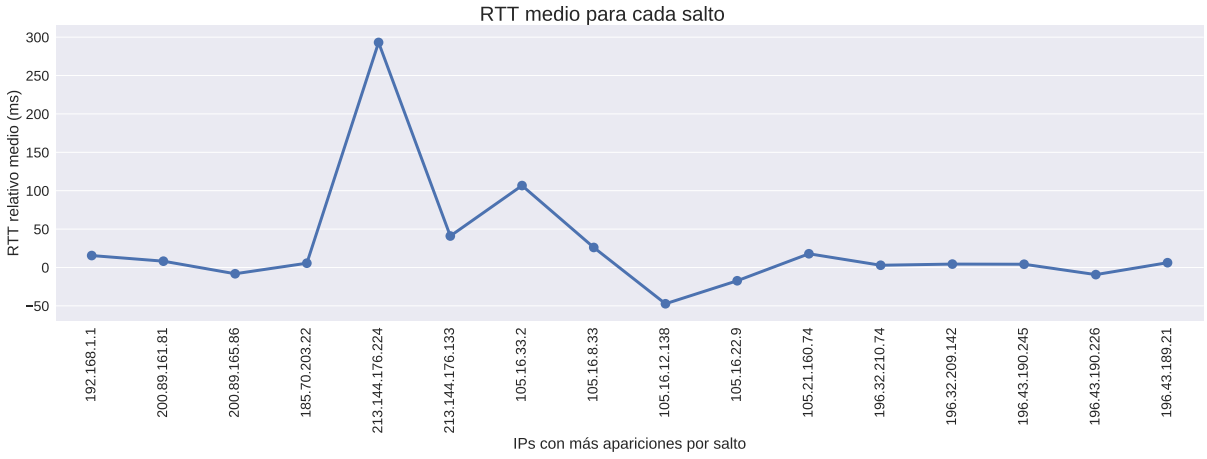

Figura 14: RTTs medios medidos para una traceroute a la Universidad Makerere

Graficamos esta ruta en el mapa de la figura **??**, donde los caminos mas rojos se corresponden con una diferencia de RTT mayor.

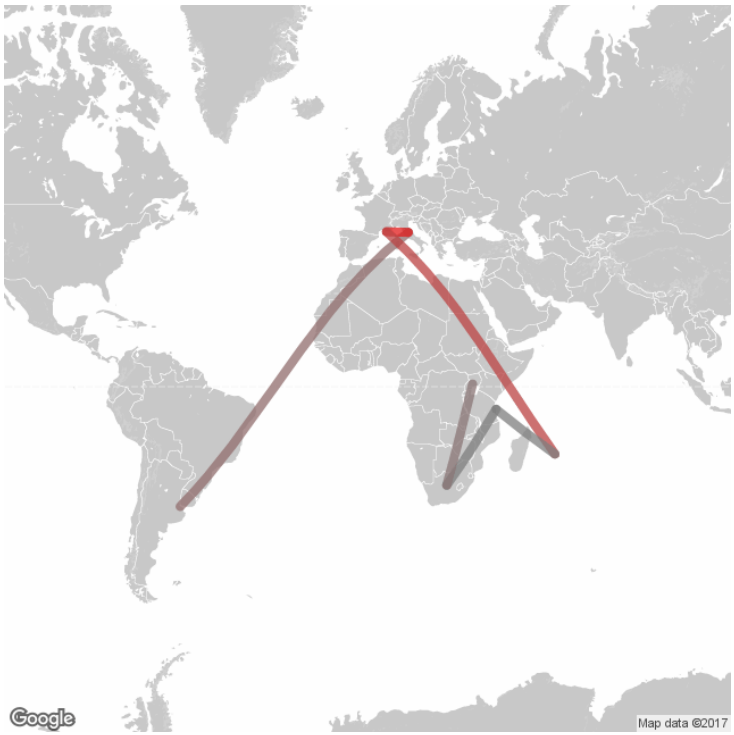

Figura 15: Mapa de ubicaciones inferidas para una traceroute a la Universidad Makerere

En total 16 de los 20 nodos del camino (**80** %) respondieron a la herramienta del traceroute.

Para terminar utilizamos el método de Cimbala para detectar cables submarinos en la ruta. El resultado, que puede verse en la figura 16 nos marca claramente el cable desde Argentina a Italia. Ademas, viendo el umbral 1 detectamos el cable que suponemos desde Italia a Mauricio y un segundo cable que debe corresponderse con el tramo Mauricio-Tanzania.

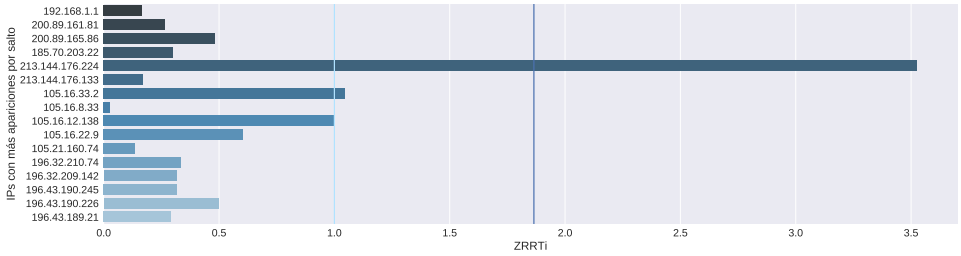

Figura 16: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

3. Conclusiones Generales

En general, todas las mediciones pudieron detectar al menos un cable intercontinental. Generalmente aquellos transoceánicos con grandes latencias. La fiabilidad de las rutas la pudimos contrastar con la implementación de Unix para traceroutes (implementada sobre UDP) y corroboramos que los resultados eran similares.

Sin embargo, pudimos notar muchas anomalías de diversos tipos.

Una de las primeras anomalías con las que nos encontramos fue que aparecían IPs de España en el tramo Argentina-Miami en la medición de Nueva Zelanda, lo cual suponemos que esté relacionado a una asignación de IPs particular del ISP. Pero esto significó, desde la primer medición, entender la falibilidad natural de cualquier herramienta de geolocalización de IPs respecto a nuestras expectativas de que el entramado final siempre sea consistente. Lo cual se profundizó a medida que fuimos encontrando nodos geolocalizados en un extremo de enlace intercontinental, pero con latencias propias del otro extremo.

Otra anomalía interesante fue que a veces los hosts destino no respondieron *echo-reply* al recibir el mensaje o nodos intermedios que no responden los *time-exceeded*. Comúnmente, esto pasa porque hay un *firewall* configurado para bloquear cierto tipo de comportamientos, en este caso de *ICMP*. Usualmente es tanto para evitar *smurf attacks (ICMP spoofing)*[5] como por motivos de performance. Lo cual quizás sea inesperado viniendo de universidades y no de empresas comerciales.

Estuvieron presentes casos de falsos negativos y falsos positivos. Después de todo, la detección de enlaces de alta latencia como outliers se trata de una técnica probabilística y puede fallar. Razones simples para que esto suceda pueden ser que existan nodos que no conforman ningún extremo intercontinental en sobrecarga (como en el caso de la medición de Londres) o predominio de rutas de larga distancia con minoría de entramado local (como por ejemplo en la de Uzbekistán) que haga que la media de los ZRTT sea alta, y por lo tanto algunos cables de alta latencia no destaquen (en el ejemplo, Argentina-Miami) y algunos cables locales tengan un alto ZRTT por su bajo RTT respecto de la media inflada.

Otro motivo de falla, más natural y esperable, es el caso de la medición de Nueva Zelanda, donde el cable submarino entre Australia y Nueva Zelanda no presenta diferencias de RTT que ameriten un outlier.

[5] https://en.wikipedia.org/wiki/Smurf_attack