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

1. Introducción **3**
1.1. ICMP Traceroute 3
1.2. Métodos 3
1.2.1. Primer ejercicio 3
1.2.2. Segundo ejercicio 3

2. Mediciones realizadas **4**
2.1. University of London 4
2.2. Victoria University of Wellington (Nueva Zelanda) 6

3. Conclusiones Generales **9**

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. 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:

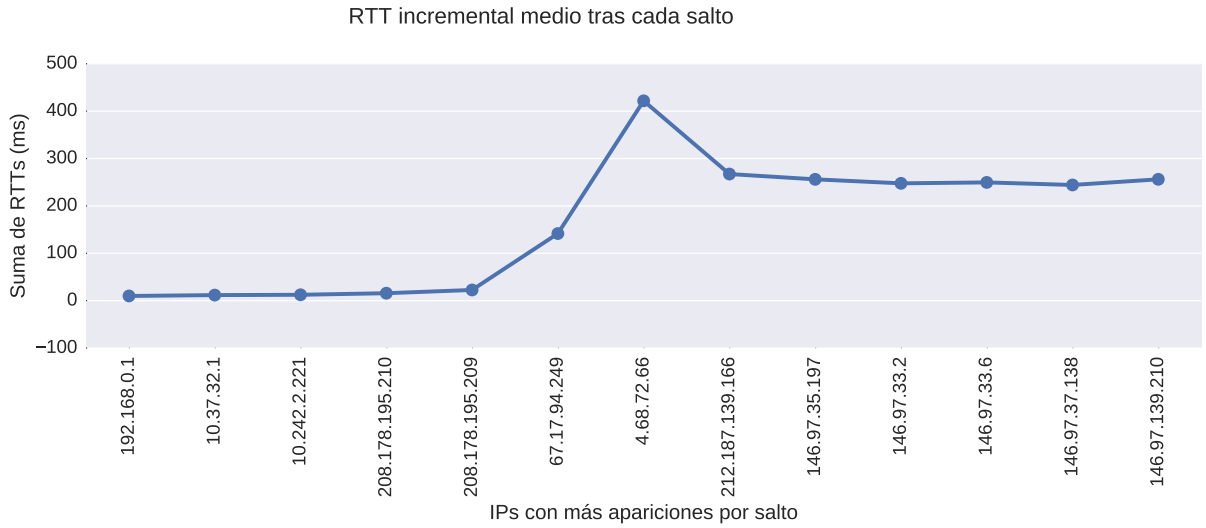

Figura 1: Comportamiento incremental de RTTs medios medidos.

Se notan dos tramos donde las diferencias entre RTTs relativos son bajas y constantes, que seguramente se corresponden al tramado interno de Buenos Aires y Londres en contraste con las rutas submarinas con mayores promedios.

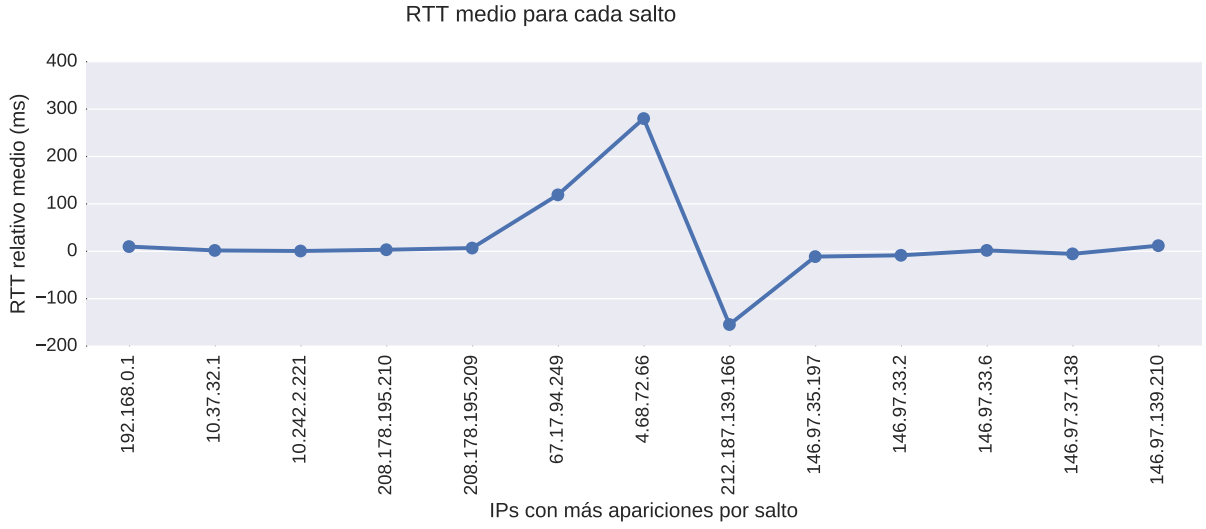

Figura 2: RTTs medios medidos para una traceroute a la Universidad de Londres.

Se pueden observar un gateway que conforma un pico, adjudicado a las IPs '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 3: 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.

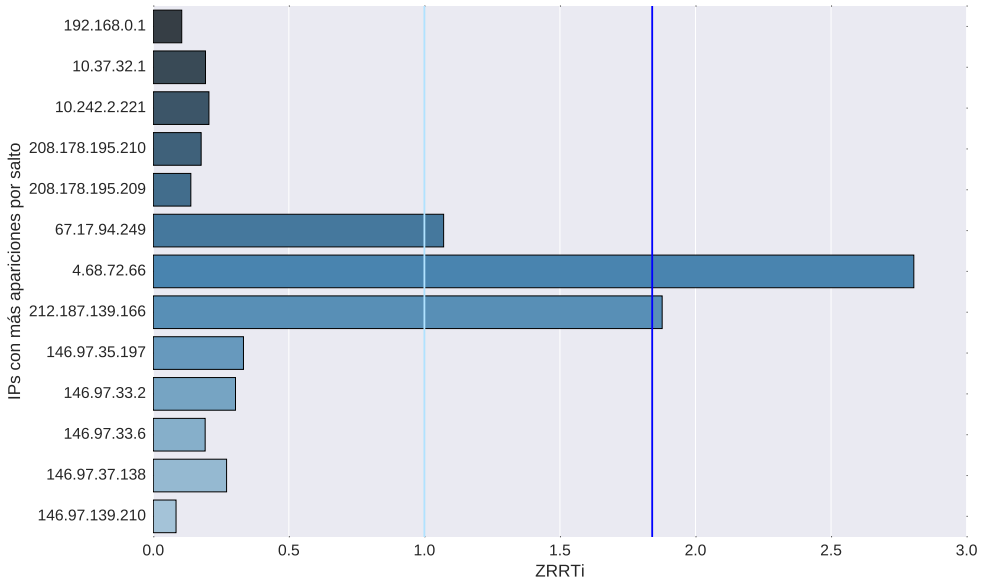

Figura 4: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

En la figura 4 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.

2.2. Victoria University of Wellington (Nueva Zelanda)

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 5.

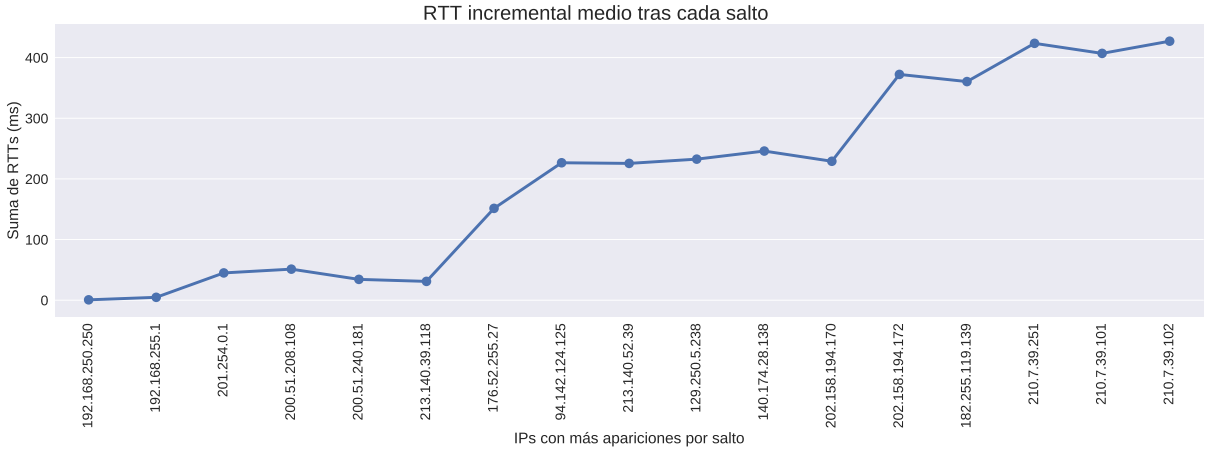

Figura 5: Comportamiento incremental de RTTs medios medidos.

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 6 se aprecian mas directamente estos tres saltos Argentina - Estados Unidos - Australia - Nueva Zelanda.

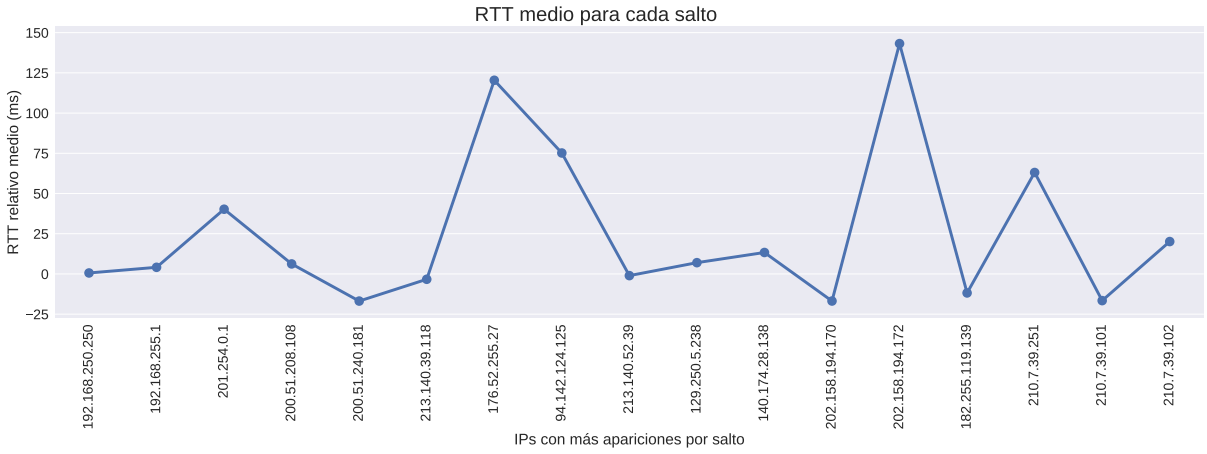

Figura 6: RTTs medios medidos para una traceroute a la Universidad Victoria de Wellington.

Vemos en el mapa de la figura 7 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.

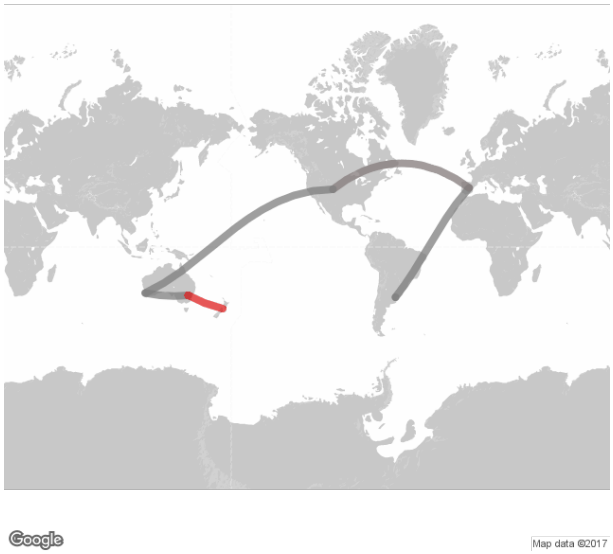

Figura 7: Mapa de ubicaciones inferidas para una traceroute a la Universidad Victoria de Wellington. Tramos con mas delay marcados en rojo.

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 2.1.

Los resultados se pueden apreciar en la figura 8. 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.

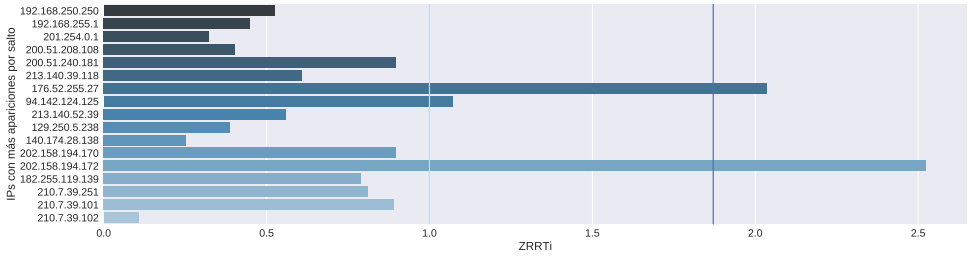

Figura 8: Outliers de la distribución ZRRTi según el método de Cimbala. En azul oscuro: valor $ZRTT_i$ correspondiente a $\tau(n)$ con n el largo de ruta y un alfa fijo (0.05 sugerido en el paper de referencia).

3. Conclusiones Generales