Detección de Enlaces Intercontinentales

Alexis Balbachan Manuel Costa Mathias Gatti

Resumen —

Index Terms —**traceroute, enlaces intercontinentales, ICMP, anomalías, RTT, TTL**

I. Introducción

— COMPLETAR —

Iniciamos este trabajo con el objetivo de aprender sobre el protocolo ARP y más en general las redes de Internet y sus algoritmos de intercambio de paquetes.

A lo largo de este informe describiremos ciertos análisis que tendrán como objetivo el modelado de emisores de información y la posterior detección de símbolos destacados. A partir de esta metodología creemos que podremos identificar dispositivos claves en la red como por ejemplo el gateway. Nuestra hipótesis es que este tendrá destacará en el intercambio de paquetes who-has siendo de los que mas reciba y envíe.

— COMPLETAR —

II. Métodos

Herramientas

Para la implementación de traceroute utilizamos el código provisto por la catedra al cual le realizamos ciertas modificaciones para poder detectar anomalías y guardar los datos obtenidos de forma más cómoda.

Detección de Anomalías

Como se describe en Cimbala[1] aplicamos un cálculo el cual compara los datos normalizados con z-score con una valor τ derivado del t-student con un α de 0.05 lo cual modela un intervalo de confianza el cual descarta los 0.025 percentiles.

Capturas

Se corrió traceroute sobre 3 universidades distintas con un ttl de 30 y 40 queries. Con el objetivo de lograr contrastar elegimos universidades muy lejanas y muy cercanas. A continuación describimos brevemente a cada una.

- Universidad de São Paulo (www5.usp.br) esta será la universidad mas cercana, ubicada en el mismo continente, por lo cual esperamos que no haya ningún enlace intercontinental.
- Universidad de Sidney (www.sydney.edu.au) escogimos esta universidad ya que nos surgió la duda de si existirá algún enlace intercontinental directo entre oceanía y america o tendrá que pasar europa resultando en varios enlaces.
- Universidad de Moscú (www.msu.ru) al estar ubicada en un punto tan alejado de nosotros estabamos seguros de que iba a haber algún salto intercontinental y quizás más.

A. Balbachan e-mail: alexisbalbachan@gmail.com
M. Costa, e-mail: manucos94@gmail.com
M. Gatti, e-mail: mathigatti@gmail.com

[1] http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/ NET-2012-08-1_02.pdf

III. Resultados y análisis

Universidad de São Paulo

Recorrido en el Planisferio

A continuación se puede ver de forma bastante clara como el paquete tuvo que pasar por estados unidos para luego ir a Europa Occidental hasta llegar finalmente a Rusia.

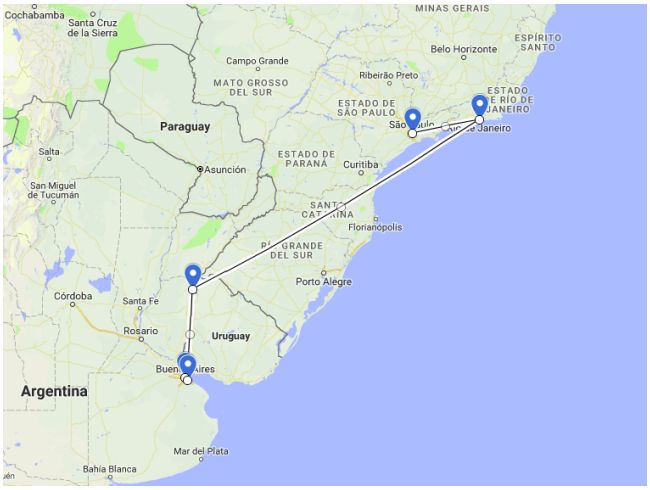

Figura 1: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio XXXXXXXXXXXXXXXXXXXXXXXXX

RTT entre saltos

A continuación intentamos ver los timepos entre saltos. Para esto calculamos la media de cada de los RTTs obtenidos de cada TTL para reducir a solo un valor las mediciones obtenidas por cada TTL.

Seguido de esto realizamos dos experimentos. Primero simplemente restamos los RTTs medios entre si como se puede ver en el primer gráfico, luego llevamos el experimento un paso mas allá normalizando con z-score los RTTs para eliminar cualquier tipo de deformación en las dimensiones del gráfico.

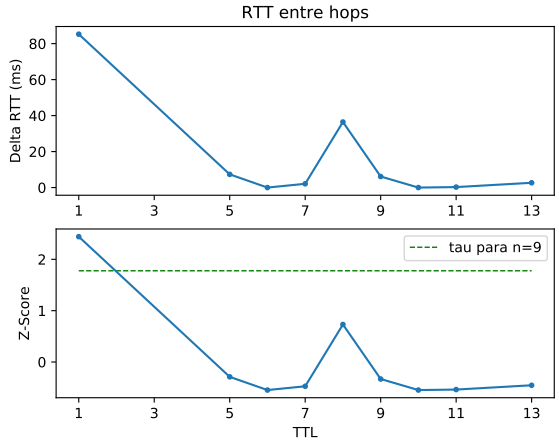

Figura 2: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio XXXXXXXXXXXXXXXXXXXXX

Como se puede observar ... COMPLETAR.

Universidad de Sidney

Recorrido en el Planisferio

A continuación se puede ver de forma bastante clara como el paquete tuvo que pasar por estados unidos para luego ir a Europa Occidental hasta llegar finalmente a Rusia.

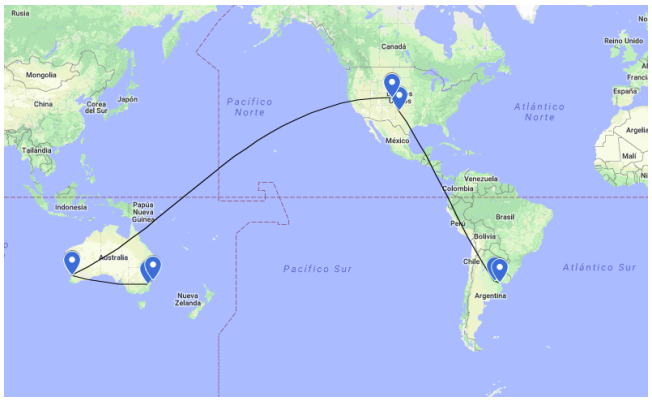

Figura 3: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio sydney.edu.au

RTT entre saltos

A continuación intentamos ver los timepos entre saltos. Para esto calculamos la media de cada de los RTTs obtenidos de cada TTL para reducir a solo un valor las mediciones obtenidas por cada TTL.

Seguido de esto realizamos dos experimentos. Primero simplemente restamos los RTTs medios entre si como se puede ver en el primer gráfico, luego llevamos el experimento un paso mas allá normalizando con z-score los RTTs para eliminar cualquier tipo de deformación en las dimensiones del gráfico.

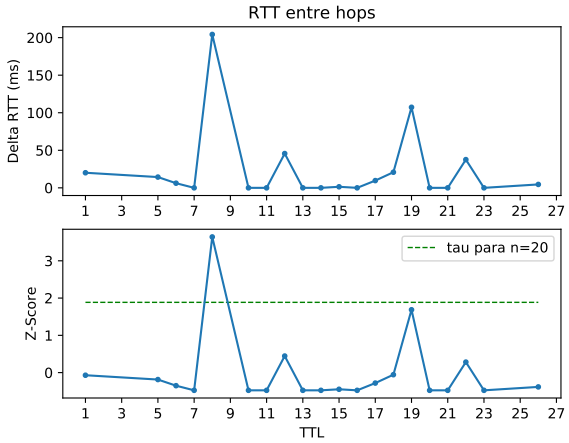

Figura 4: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio sydney.edu.au

Como se puede observar ... COMPLETAR.

Universidad de Moscú

Recorrido en el Planisferio

A continuación se puede ver de forma bastante clara como el paquete tuvo que pasar por estados unidos para luego ir a Europa Occidental hasta llegar finalmente a Rusia.

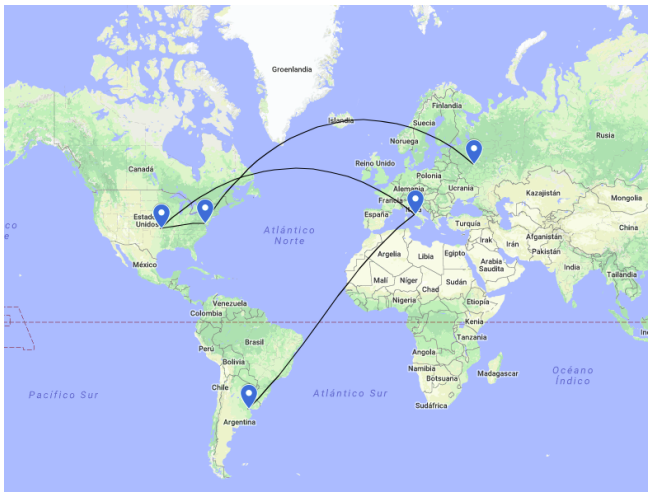

Figura 5: Recorrido realizado por los paquetes durante la ejecución de traceroute al intentar alcanzar el sitio www.msu.com

RTT entre saltos

A continuación intentamos ver los timepos entre saltos. Para esto calculamos la media de cada de los RTTs obtenidos de cada TTL para reducir a solo un valor las mediciones obtenidas por cada TTL.

Seguido de esto realizamos dos experimentos. Primero simplemente restamos los RTTs medios entre si como se puede ver en el primer gráfico, luego llevamos el experimento un paso mas allá normalizando con z-score los RTTs para eliminar cualquier tipo de deformación en las dimensiones del gráfico.

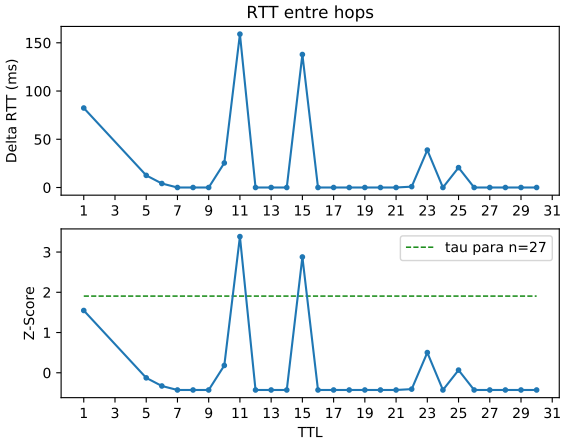

Figura 6: RTT entre saltos (antes y después de normalizar respectivamente) para el sitio www.msu.com

Como se puede observar ... COMPLETAR.

IV. Discusión

Como resultado final pudimos identificar de distintas maneras nodos destacados, por ejemplo a partir del grafo subyacente que armamos pudimos identificar en todos los casos al gateway a partir del nodo de mayor grado. A continuación describimos brevemente cada caso analizado por separado.

.1 São Paulo

En la red domiciliaria se pudo ver en el grafo resultante como destacaban dos nodos. Uno de ellos, el de mayor grado, era el gateway, el otro creemos que fue la computadora que tomó las mediciones ya que estaba accediendo a multiples sitios de internet lo cual provoco un gran intercambio de paquetes.

.2 Sidney

Este es el grafo mas grande y en el cual se vuelve aún mas claro el patrón que veniamos viendo, el nodo 10.2.203.254 resalta completamente de los demás y concuerda perfectamente con nuestra hipótesis de que el gateway es el que mas paquetes intercambia en este protocolo, lo cual lo vuelve un nodo destacado.

.3 Moscow

Quizas por una mala configuración de la red o por la poca clientela que había en este local en el horario en que se tomaron las mediciones (7:10 AM) es que este grafo resultó ser tan pobre, de todas maneras se pueden observar perfectamente los dos nodos que uno esperaría ver como minimo. El gateway y la computadora que tomo las mediciones.