Rutas en redes: Utilizando traceroute y métodos estadísticos para detectar enlaces submarinos

Gonzalo Ciruelos Axel Maddonni Federico Patané Gabriel Thibeault

***Resumen*—En este trabajo implementaremos una herramienta para trazar la ruta de paquetes ICMP, es decir un `traceroute`. Además, utilizando los tiempos de los RTT de los paquetes, desarrollaremos un método estadístico para detectar los enlaces submarinos.**

***Index Terms*—traceroute, enlaces submarino, ICMP, RTT, IP**

I. Introducción teórica

En este trabajo nos proponemos usar un traceroute junto con herramientas estadísticas para intentar detectar enlaces submarinos en las rutas IP.

Nuestra implementación de traceroute se basará en paquetes ICMP de tipo `echo request`. Enviaremos, al destino especificado, paquetes ICMP echo request con distintos TTL, esperando que el paquete se quede sin tiempo en un nodo intermedio, y este nodo intermedio nos mande otro paquete ICMP (esta vez de tipo `time exceeded`) y de esta manera sabremos la dirección IP del nodo intermedio.

Más adelante introduciremos más en detalle cómo fue hecha la implementación de traceroute. Sin embargo, lo que más nos interesa del traceroute es el RTT entre cada nodo: como podemos tomar el tiempo que tarda un paquete en ir y volver de cada nodo intermedio de la ruta, podemos estimar el tiempo que tarda el salto entre cada nodo de la ruta. De esta manera, como nuestro objetivo es detectar enlaces submarinos, podemos pensar que una buena forma de detectarlos sería detectar cuando el salto tarda mucho.

Esto es efectivamente lo que haremos, tendremos una variable aleatoria que será el RTT relativo, es decir, entre saltos, y tomaremos todos los RTT relativos de nuestro traceroute como muestras de esa variable aleatoria. Luego, usando algún modelo de detección de outliers, intentaremos detectar mediciones que corresponden con enlaces submarinos.

Como método de detección de outliers utilizaremos el método descripto en [2]. Este método se basa en normalizar la variable aleatoria, para obtener una nueva variable aleatoria que llamaremos ZRTT. Es decir, supondremos que RTT rel (los RTT relativos) son una $N(\mu, \sigma)$ para algún μ, σ y normalizaremos para obtener una $N(0,1)$.

G. Ciruelos e-mail: gonzalo.ciruelos@gmail.com
A. Maddonni, e-mail: axel.maddonni@gmail.com
F. Patané, e-mail: fedepatane20@gmail.com
G. Thibeault, e-mail: gabriel.eric.thibeault@gmail.com

$$ZRTT = \frac{RTT_i - \overline{RTT}}{s_{RTT}}$$

Notar que sin embargo este método es imperfecto, porque la variable aleatoria podría no ser (y de hecho no es) una normal.

Ahora bien, tenemos que elegir algún valor límite tal que si $ZRTT$ es mayor que ese valor, diremos que es un outlier, y en consecuencia ese enlace es un enlace submarino. Aquí, es donde el paper [2] propone utilizar la variable τ de Thompson. La τ de Thompson se calcula como sigue

$$\tau = \frac{t_{\frac{\alpha}{2}}(n-1)}{\sqrt{n}\sqrt{n-2+t_{\frac{\alpha}{2}}^2}}$$

Donde n es la cantidad de mediciones.

Todo esto resume la parte teórica del problema. De aquí en adelante nos adentraremos en la implementación de la herramienta, y en la experimentación.

II. Desarrollo

Como explicamos anteriormente, ...

A. Primera consigna

B. Segunda consigna

Cabe destacar que en el cálculo de los ZRTTs, sólo tomamos valores no-negativos[1] de los RTTs entre saltos. Sin embargo, en los gráficos de RTTs que presentamos, los valores pueden ser menores a 0. De forma contraria las figuras proveen información confusa y difícil de interpretar.

C. Conceptos generales

D. Université de Laval

A continuación presentamos los los gráficos resultantes de realizar una *traceroute* a la página de la Université de Laval[2].

[1] Consideramos como 0 a los valores negativos.
[2] www2.ulaval.ca.

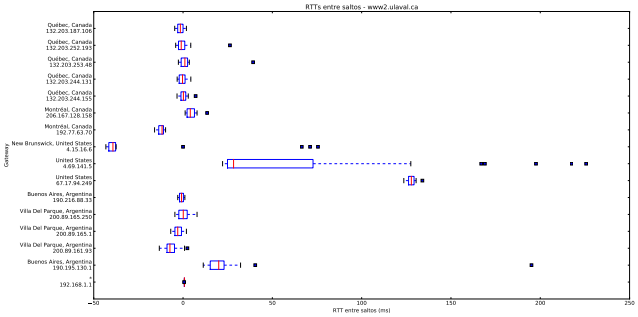

Figura 1

RTTs entre saltos. El valor asignado al i-ésimo nodo corresponde al salto entre el i-ésimo y el $i-1$-ésimo nodo. Para el primer nodo se utiliza simplemente su RTT.

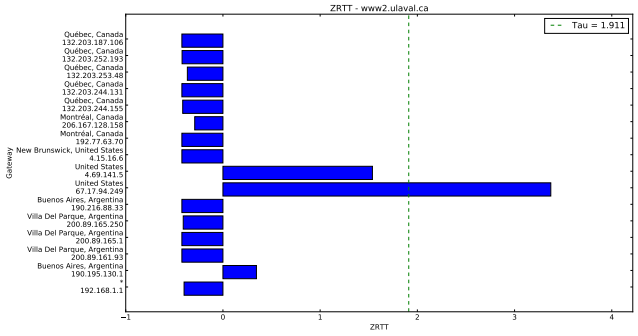

Figura 2

ZRTTs entre saltos.

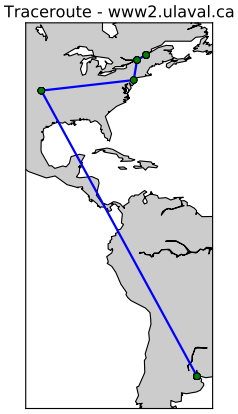

Figura 3

Ubicación geográfica estimada de la ruta tomada.

En la realización de la *traceroute*, 6 de los 22 ($27.\overline{27}\%$) nodos no respondieron los *Time exceeded*.

Sólo un salto (de 190.216.88.33 a 67.17.94.249) se presentó como *outlier* según el método planteado. De acuerdo a la estimación geográfica, este salto se da entre Buenos Aires y Estados Unidos, y efectivamente coincide con el único enlace intercontinental de la ruta.

III. Conclusión

Referencias

[1] Scapy
http://www.secdev.org/projects/scapy
[2] Outliers - Cimbala, J.
http://www.mne.psu.edu/cimbala/me345/Lectures/Outliers.pdf