Análisis de tráfico de redes locales usando Teoría de la Información

Alexis Balbachan Manuel Costa Mathias Gatti

***Resumen*—**

***Index Terms*—entropía, Teoría de la informacin, ARP, LAN, unicast, broadcast, sniffing**

I. Introducción

II. Métodos

Herramientas

Para la captura de tráfico se utilizó el módulo de manipulación de paquetes *Scapy* para python, el cual provee una interfaz sencilla para nuestros requerimientos puntuales. *Scapy* permite la captura y posterior guardado de paquetes en una red, para luego ser filtrados, inspeccionados o manipulados con facilidad. Además, para incrementar la cantidad de paquetes vistos por un host, se activó el modo promiscuo o modo monitor en sus respectivas interfaces de red.

Modelo de las fuentes

Fuente S1

Dado el tráfico de capa 2 obtenido en cada captura, se modeló una fuente de memoria nula S1 = $\{s_1, s_2, s_3, ..., s_n\}$ donde cada s_i está formado por una tupla ¡broadcast—unicast, protocolo capa 3¿.

Fuente S2

Igualmente que S1, se modeló la fuente de memoria nula S2 con el objetivo utilizando sólo las direcciones IP dentro de paquetes de protocolo ARP con el objetivo de poder distinguir los hosts de cada red. En este caso se consideraron diversas opciones para el modelado de la fuente, donde cada s_i representaba las direcciones IP de los hosts, aunque su contabilización se regía por si la dirección aparecía en los campos:

- Fuente o Destino
- who-has Fuente
- who-has Destino
- is-at Fuente
- is-at Destino

Capturas

Se hicieron 3 capturas en redes diferentes de 10000 paquetes cada una:

- Red hogareña mediana, con aproximadamente 10 usuarios, se utilizó una interfaz ethernet.
- Red pública grande, en este caso se capturó mediante una interfaz wifi el tráfico del laboratorio de informática de la universidad.
- Red pública grande, también mediante la interfaz wifi, se capturó el tráfico en un Starbucks.

III. Resultados y análisis

Red hogareña

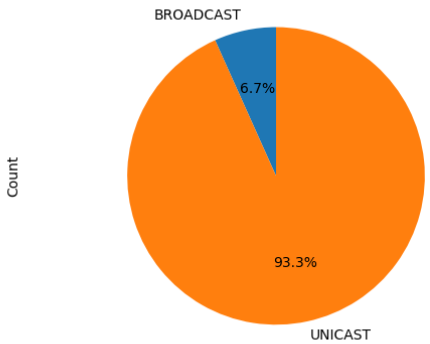

Figura 1
Proporción de paquetes unicast/broadcast en la captura

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

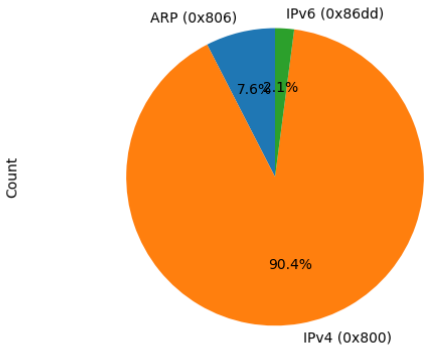

Figura 2
Proporción de protocolos en la captura

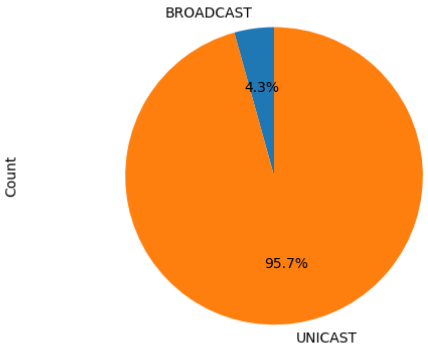

Figura 4
Proporción de paquetes unicast/broadcast en la captura

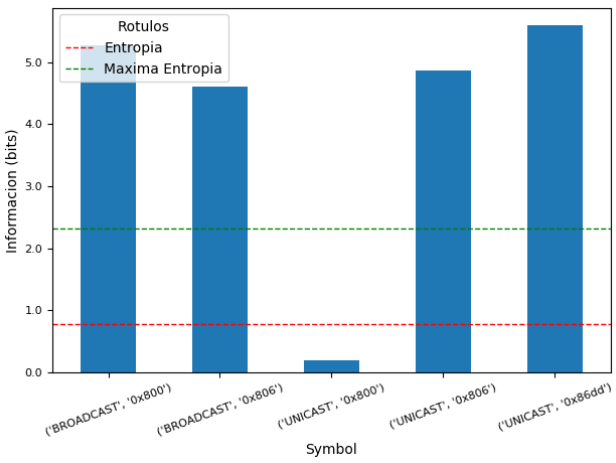

Figura 3
Información de los símbolos de la fuente S1, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

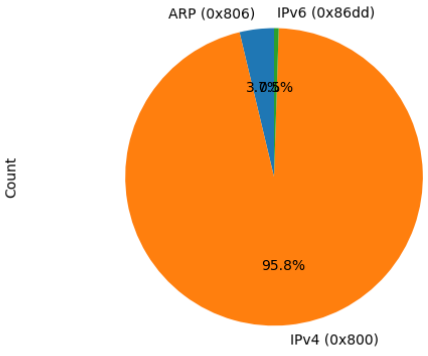

Figura 5
Proporción de protocolos en la captura

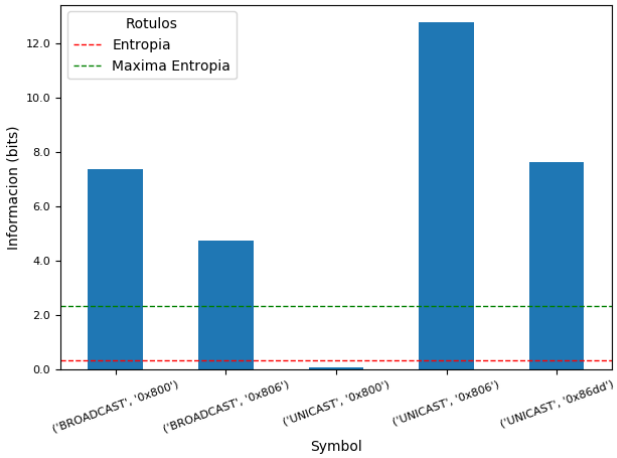

Figura 6
Información de los símbolos de la fuente S1, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

Red Starbucks

IV. Discusión