Wiretapping de paquetes ARP: analizando redes locales usando Teoría de la Información

Gonzalo Ciruelos , Axel Maddonni y Federico Patané

***Resumen*—Con el objetivo de comprender diversos aspectos de una red local, nos planeteamos analizar sus paquetes ARP usando herramientas de la teoría de la información. Para lograr eso, modelamos algún aspecto de nuestra red como una fuente de inforamción, de manera de poder analizarla con las herramientas previamente dichas. Además, comparamos distintos tipos de redes para poder confirmar o refutar nuestras hipótesis generales.**

***Index Terms*—ARP, LAN, broadcast, unicast, entropía, información, Ethernet, Wi-Fi**

I. Introducción teórica

En este trabajo nos proponemos utilizar herramientas de la Teoría de la Información y los paquetes ARP para intentar comprender diferentes redes locales. La pregunta que nos intentaremos responder en este trabajo es ¿Podemos conocer la topología de la red y/o sus nodos más importantes?

La explicación de las fuentes utilizadas vendrá más adelante, pero es pertinente presentar el formato de los paquetes ARP. El protocolo de resolución de direcciones (Address Resolution Protocol) [1] es un protocolo usado para la resolución de direcciones de la capa de red a direcciones de la capa de enlace (usualmente MAC), lo que es una función crítica en redes de múltiple acceso.

Un paquete ARP tiene muchas partes, pero la que más nos interesa es el campo OPER, o sea el campo de Operación, que nos indica qué función cumple ese paquete. Los distintos valores de OPER en paquete ARP son is-at y who-has. Un paquete who-has es un paquete broadcast en el que una computadora pregunta al resto de la red quién es la que tiene una dirección de capa de red (generalmente IP) dada. La respuesta a ese paquete es un paquete is-at, que es un paquete unicast, enviado desde la computadora con la dirección de capa de red requerida hasta la computadora que emitió el who-has.

Por otro lado, con respecto a la teoría de la información, utilizaremos los conceptos de información y entropía clásicos.

II. Desarrollo

Como explicamos anteriormente, el trabajo se basará en analizar redes locales capturando paquetes ARP de redes locales y analizandolos utilizando herramientas de la teoría de la información.

Para capturar los paquetes de la red analizada, utilizamos el programa Wireshark. Luego, para postprocesar los datos y computar la inforamación pedida utilizamos la librería de Python Scapy. Scapy es una poderosa herramienta que permite capturar, decodificar, crear y envíar paquetes de manera muy sencilla.

A. Ejercicio 1

El ejercicio 1 proponía analizar los resultados modelando a los paquetes como una fuente de información muy simple: simplemente distinguir entre paquetes broadcast y paquetes unicast. La fuente consiste en dos símbolos, uno que representa a los paquetes unicast, y otro que representa a los paquetes broadcast.

Esta fuente no nos permitirá conocer muy bien quién es quién en la red, pero nos dará quizás un poco de información sobre lo que está pasando en la red local.

Que la cantidad de mensajes de broadcast sea muy grande, o sea, la información del símbolo que representa a los mensajes broadcast sea muy chica, será lo esperado. Esto se debe a que en una red normal, en la cual podemos escuchar todo lo que está pasando, lo esperable es que los dispositivos se comuniquen unos con otros en vez de estar envíando broadcasts todo el tiempo.

De alguna manera, si vemos pocos paquetes unicast, o sea que la información de este símbolo es muy alta, puede significar dos cosas:

1. No tenemos visibilidad total de la red, por ejemplo porque está switcheada, y entonces vemos solo los paquetes unicast dirigidos a nuestro host.
2. No hay comunicación efectiva entre los hosts de la red, porque los paquetes unicast de alguna manera miden cuanta comunicación de un host a otro está sucediendo.

Nuestra implementación de este ejercicio puede verse en el archivo `ejercicio1.py`.

B. Ejercicio 2

El ejercicio 2 prop

Nuestra implementación de este ejercicio puede verse en el archivo `ejercicio2.py`.

III. Experimento 1

IV. Experimento 2

Referencias

[1] RFC 826 - Ethernet Address Resolution Protocol `http://tools.ietf.org/html/rfc826` C. Plummer 1982

[2] `http://www.secdev.org/projects/scapy`

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

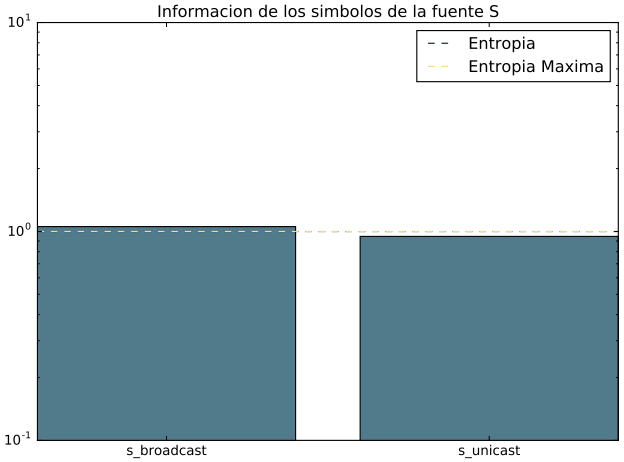

Figura 1

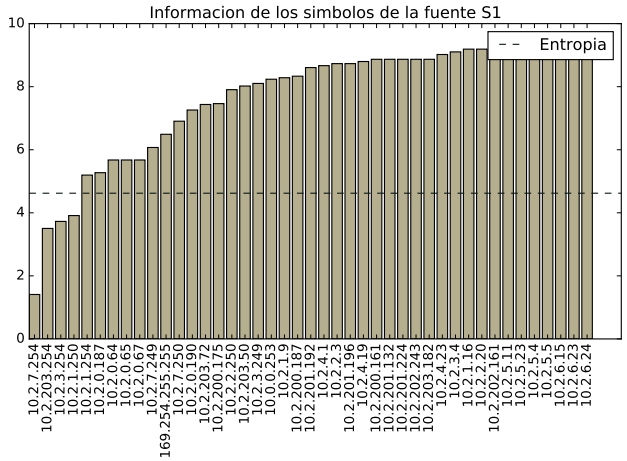

Figura 3
Información de los símbolos de la fuente S1: solamente los nodos con menor información son representados.

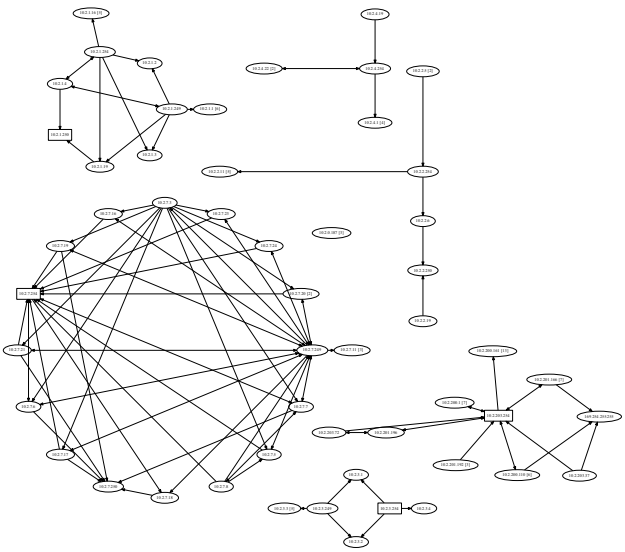

Figura 2
Grafo de conectividad de la red, inferido de los paquetes who-has. Para ver con mayor detalle, se puede hacer zoom-in en el pdf.

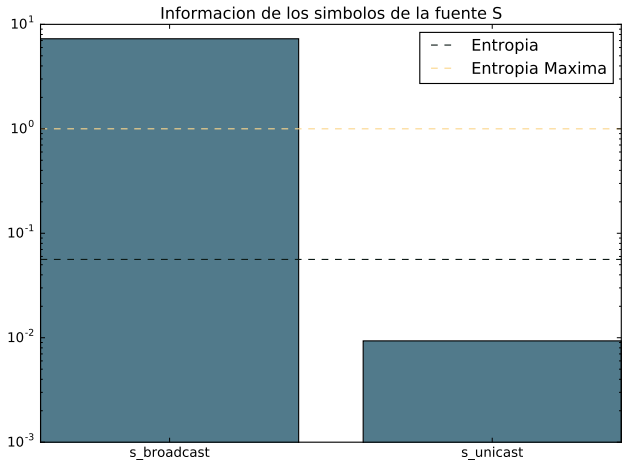

Figura 4

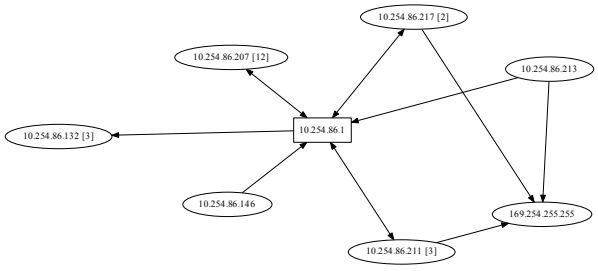

Figura 5
Grafo de conectividad de la red, inferido de los paquetes who-has. Para ver con mayor detalle, se puede hacer zoom-in en el pdf.

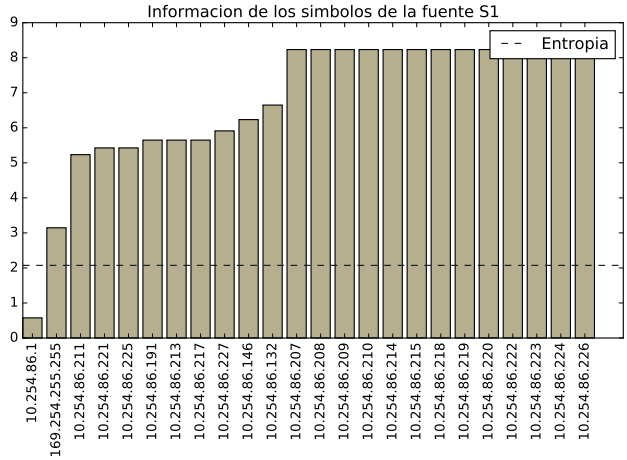

Figura 6
Información de los símbolos de la fuente S1: solamente los nodos con menor información son representados.