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 planteamos 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

BLAH

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