DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

TP1: Wiretapping

20 de abril de 2016

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Benitti, Raul	592/08	raulbenitti@gmail.com
Castro, Damian	592/08	ltdicai@gmail.com
Lizana, Helen	118/08	hsle.22@gmail.com
Grenier, Michelle	418/10	michelle.grenier@hotmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

1. Introducción

Las redes de computadoras han dejado de ser una tecnología reservada a ciertos ambitos científicos y militares para convertirse en piezas fundamentales en el desarrollo de casi cualquier actividad, a tal grado que las relaciones humanas, desde el comercio hasta las guerras, han sido profundamente transformadas por la conectividad alcanzada en los últimos años. Es por esto que analizar los distintos aspectos de una red puede proveer información útil para comprender el uso que se esta dando a la red, informacion que sirve tanto para modificar la infrastructura y los protocolos utilizados a fin de mejorar la calidad del servicio como, incluso, manipular las actividades que se esten llevando sobre ella.

En el presente trabajo observaremos sistemas basados en dos de las tecnologías de redes más difundidas, Ethernet y WiFi 802.11, y analizaremos los datos obtenidos utilizando dos modelos de fuente de información para sacar conclusiones sobre el uso y la configuración de las redes.

1.1. Información y Fuente de información

Una fuente de información es todo aquello que emite mensajes de acuerdo a una ley de probabilidad fija. Los mensajes pertenecen a un conjunto finito de símbolos $S = s_1, ..., s_n$, conocido como el alfabeto de la fuente. La emisión de un símbolo s_i por parte de la fuente S representa un evento que tiene asociada una probabilidad fija $P_S(s_i)$ de ocurrir.

Dado un evento e con probabilidad $P(e)$, se define la **información del evento** e como

$$I(e) = -\log P(e)$$

$I(e)$ es una medida de la cantidad de información que obtenemos por la ocurrencia de E: mientras más improbable sea E, mayor será la información brindada por su ocurrencia (menor sera la incertidumbre sobre el hecho observado). Dicho de otra manera, si sabemos que un evento E tiene alta probabilidad de ocurrir, entonces su ocurrencia no aportará mucha información sobre lo que se esta observando.

1.2. Entropía

Dada una fuente de información $S = s_1, ..., s_n$, se define la entropía de S, $H(S)$, como la suma ponderada de la información de casa simbolo de S

$$H(S) = \sum_{i=1}^{n} P(s_i) * I(s_i)$$

La entropía de una fuente de información mide la cantidad de información esperada al observar la emisión de un nuevo símbolo por parte de la fuente. Dado un evento e

1.3. ARP

Para poder realizar un envío de paquetes de capa 3 utilizando los servicios de capa 2, es necesario poder asignar un mapeo entre las direcciones de ambas capas. ARP (*Address Resolution Protocol*) es un protocolo de control que surge como respuesta a esta necesidad. Cada host y switch de una red mantiene una tabla ARP donde se relaciona una dirección lógica d con la direccion física f a la que debe entregarse

cualquier paquete destinado a d (el host con direccion física f no es necesariamente el destinatario de la dirección d: puede ser un intermediario que sabe como hacer llegar el paquete a d). En el caso de redes IP sobre Ethernet, ARP es utilizado para mapear direcciones IP con direcciones MAC. La configuracion de estas tablas ARP se realiza dinámicamente siguiendo un protocolo que consiste básicamente en los siguientes pasos:

1. Un host **A** desea enviar un paquete a una determinada IP. Si **A** conoce la direccion MAC a la que debe enviar los paquetes destinados a esa IP, entonces utiliza esa direccion física. Si no, envía un mensaje broadcast dentro de la red (en Ethernet, MAC destino = FF:FF:FF:FF) y aguarda la respuesta. Este mensaje se conoce como **ARP request**, y lleva la siguiente información:

   asad.

2. Si dentro de la red existe un host B que sabe como direccionar a la direccion IP requerida, entonces responde al mensaje **ARP request** con un mensaje **ARP reply** indicando su dirección física. Este host puede ser el dueño de la dirección IP, o un host intermediario (como un router). Además, actualiza su tabla ARP para relacionar la

3. **A** recibe el ARP reply de **B**, actualiza su cache y envía el paquete original utilizando la dirección física de **B**.

En este informe mostraremos como podemos utilizar la información provista en los paquetes ARP para analizar la topología de una red.