DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

TP1: Wiretapping

Teoría de las Comunicaciones
Segundo Cuatrimestre 2016

Integrante	LU	Correo electrónico
Cravero, Marcos	495/15	marcoscravero2175@gmail.com
Mignanelli, Alejandro Rubén	609/11	minga_titere@hotmail.com
Suárez, Federico	610/11	elgeniofederico@gmail.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

En el presente trabajo se utilizarán técnicas provistas por la Teoría de la Información para distinguir diversos aspectos de la red de manera analítica, en particular, los paquetes broadcast de la red, y los nodos distinguidos(Se puede pensar que un símbolo es distinguido cuando sobresale del resto en términos de la información que provee). Para esto se realizarán capturas de paquetes en 3 redes distintas modelando dichos paquetes con diferentes fuentes de información, S y S_1, que se detallarán a continuación:

- Fuente S:

  Sean $p_1..p_i$ los paquetes que se capturan en un enlace. Podemos conocer los destinos a los que están apuntados los paquetes que encapsulan la información con el campo dst del frame de capa de enlace. Se pueden modelar los paquetes capturados como una fuente de información binaria de memoria nula S, definiendo el conjunto de símbolos que emite como $S_{BROADCAST}$, $S_{UNICAST}$. Si se captura un paquete p en un intervalo de tiempo [t_i,t_f], se dice que S emite $S_{BROADCAST}$ si $p.dst$ == ff : ff : ff : ff : ff : ff, y si no emite $S_{UNICAST}$. Esta fuente distingue entre mensajes Broadcast y Unicast que aparecen en la red en ese intervalo.

- Fuente S_1:

  Con el objetivo de distinguir los nodos (hosts) de la red se utilizará una fuente de información de memoria nula S_1 que estará basada sólo en las direcciones IP de los paquetes ARP. En principio se tienen 3 opciones: tener en cuenta sólo las IPs destino, sólo las IPs origen o la combinación de ambas. Dado que se quieren distinguir los nodos de la red, se necesitaría que los símbolos de la fuente sean tales nodos, o más bien sus IPs. Con esto dicho, la tercera opción queda descartada ya que implicaría que los símbolos de la fuente sean combinaciones de pares de IPs. En el proyecto se analizarán las dos primeras alternativas, y se llegará a una conclusión de cual es la más conveniente para nuestro objetivo.