Assignment 3

CS 407

Due April 17, 2013 In Class

1 Introduction

The goal of this project is to become familiar with Wireshark and perform an analysis of a wireless packet trace. Wireshark is a GUI tool which shows packets that have been sent/received on a given network interface. It is often useful for debugging networking problems. For this assignment we will provide a packet capture file in which you will perform your analysis. Some questions can be answered using Wireshark's filters, but you will most likely need to write a script/C program to answer some questions (see Libraries).

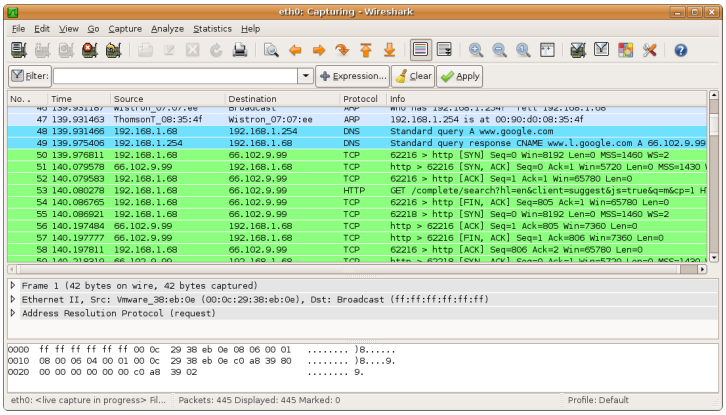

Figure 1: Screenshot of Wireshark (`http://en.wikipedia.org/wiki/File:Wireshark_screenshot.png`)

2 Questions

Download the PCAP file (found here: `http://cs.wisc.edu/~griepent/cs407/trace.pcap.zip`), and answer the following questions:

1. What ESSIDs do you observe in beacon frames?
2. What channel was this capture taken on?
3. What is the average beacon interval for each of the ESSIDs?
4. How many MAC addresses do you see communicate with bssid "00:24:6c:5e:03:30"?
5. List all the management frames you observe in the trace and indicate how many you observe of each type?

6. What is the highest data rate you observe in the trace? What does this indicate regarding the channel width used and the 802.11 standard (g,n, etc)?

7. What data rate are management frames sent at for bssid "00:24:6c:5e:03:30"? Why?

8. From the trace, estimate how many packet transmissions were not correctly received at each intended receiver?

9. What is the estimated fraction of data frames that were sent with and without RTS/CTS in this entire trace? Note that you may not hear both parts of an RTS/CTS.

10. From the entire trace, calculate what fraction of time there was an packet being physically transmitted on the air? This is the airtime utilization of the channel. The total duration of the trace is available in the trace.

Be sure to explain how you arrived at each answer. If you wrote a program/script, provide a high-level explanation of what your program did.

3 Libraries

Here are some potential libraries you can use to parse pcap files. Please note, you may not have sufficient permissions to install/run the Python/Ruby library on CSL machines, but libpcap is supported. Libpcap is a C library which can be used by adding the $-lpcap$ flag when you compile. Sample usage can be found here: `http://dog.tele.jp/winpcapeng/html/group__wpcap__tut7.html`

Library Links:

- `http://www.tcpdump.org/` (C)
- `http://www.secdev.org/projects/scapy/` (Python)
- `https://github.com/shadowbq/pcaprub` (Ruby)

An alternative (and simpler) approach is to export the pcap file as a CSV file, and process the packet capture that way. Select "File" → "Export Packet Dissections" and select "CSV" in Wireshark. This will only export what is displayed on the top half (not the entire packet), so you need to ensure that relevant fields are shown as a column. To do this, click on a field in the packet dissection (i.e., SSID of a beacon frame), right-click and select "Apply as Column".

4 Grading

Each question will be worth 10%.

5 Collaboration Policy

This assignment must be done individually.

6 Handin

Handin a written/typed copy with answers at the beginning of class on the 17^{th}.