UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

EEC173B/ECS152C **Spring 2005**

Mini-Project #1 (Due May 4)

1. Discovering Davis Wireless Coverage (10%)

   As discussed in the first lab, before Intel Placelab software can be used to "estimate" user location, we need to populate the wireless coverage database with the different wireless networks discovered in the particular area, or stumbling. Stumbling is the process of collecting traces of available beacons like 802.11 access points on a mobile device which is also connected to a GPS unit. You will be provided with a GPS receiver. You can choose to perform the network stumbling with your laptop (recommended), PDA, or phone. Please follow the following procedures:
   - Register with Wireless Geographic Logging Engine (WiGLE) at http://www.wigle.net
   - If you are using a laptop, download NetStumbler from: http://www.stumbler.net/
     If you are using a PDA, download MiniStumbler from: http://www.stumbler.net/
     If you are using a cell phone, follow the PlaceLab Phone Stumbler Howto at: http://www.placelab.org/toolkit/doc/phonestumbler_howto/
   - Sign up for a specific quadrant of Davis that your team is going to explore (to avoid duplication with other teams).
   - Happy stumbling!
   - Post your files to www.wigle.net and submit a summary table of wireless networks discovered and their GPS location in your report

   In your report, answer the following questions:

   (a) The Global positioning system (GPS) is funded and controlled by the U.S. Department of Defense. Explain how it works. For example,
   - How many satellites is in the system? These satellites orbit the Earth at what distance?
   - How do we track/monitor these satellites?
   - How does a GPS receiver compute the four dimensions- x, y, z coordinates of position, and the time?

   (b) What are the factors that influence the accuracy of location estimation using GPS? How can you improve the accuracy?

   (c) What are the alternate approaches to track locations that cannot be reached by GPS?

2. Sniffing the wireless links (Bonus 5%)
   You can examine the details of network conversations using a tool called a network protocol analyzer. A network protocol analyzer is a piece of software that can record each packet sent over the network and display them in a human-readable format. On a busy network, this can be a lot of information so network protocol analyzers typically provide summary statistics about all packets and allow users to filter out unwanted data or search for specific packets of interest.

   You will learn the most from this exercise if you install Ethereal and Kismet on your local computer.
   - Ethereal is available for most platforms, including Windows, Mac, and Unix/Linux. You can install the latest version directly from the Ethereal website, http://www.ethereal.com
   - For wireless networks, you need to put the wireless network interface into promiscuous mode and capture it with open source application called Kismet, which can be downloaded from: http://www.kismetwireless.net. Traces taken with kismet can still be viewed in Ethereal.

   In this experiment, we explore aspects of IEEE 802.11 traffic in general and we illustrate the difference between a network without WEP enabled and with WEP enabled.

   Answer the following questions:
   (a) What percentage of the packets are beacons? What percentage of data sent? How do you know?

   (b) If you know the MAC address of the access point, an FTP server, and the legitimate client. Write a filter to find any other MAC addresses present in the trace.

   (c) Search for estimates of how far away from a wireless access point you can go in a typical home or office environment. How about in the open?