CIS6930/4930 Mobile Networking - Spring 2009

Mobile Networking Experiment #1

Due Date: Monday, March 23, 2009

Start Date: February 24, 2009

Abstract

The goal of this lab experiment is to investigate the underlying assumption of Mobile Node (MNs) encounters in Bluetooth and Wireless LAN (WLAN) networks, and to develop fundamental understanding of realistic user behavior to communicate information. In the WLANs, MNs connect and disconnect with several Access Points (APs) intermittently as opposed to the always-on nodes. In a big WLAN deployment such as university campuses, this activity happens among severals APs with thousands of MNs together. An encounter event among MNs has the following assumption: The MNs can communicate with each other directly if they are associated with the same AP or the same switch port (as in USC trace) at the same time. The duration of an encounter between two or more MNs is the overlapped time intervals derived from WLAN traces.

In Bluetooth, encounters occur more explicitly, when two or more MNs converge in their individual transmission range. Bluetooth matches very closely to MNs movement (people's movement), as it typically has a short range (10 meters). However, typical Bluetooth encounter between a pair of devices is for a very short duration as compared to WLAN encounter. Thus, a true Bluetooth encounter can be defined as a minimum threshold time required to perform some activity.

There are two set of experiments to be done: In one part of the experiment, teams will analyze Bluetooth encounters and in later part, they will analyze WiFi encounters. In Bluetooth experiment, the teams will gain hands-on experience to explore the chances for inter-device communication through collecting Bluetooth encounter traces, post-processing and analyzing the traces, comparing it with other encounter traces and brain storming on how to utilize this encounter information in delay tolerant networks (DTNs). They will also investigate the intensity and duration of encounters.

In WiFi experiment, the teams will gain hands-on experience to explore the possibility for inter-device communication through collecting WiFi encounter traces and investigating the assumption that if two MNs logged in at the same time under the same AP, have a valid encounter. They will also do brainstorming on how to utilize this encounter information in delay tolerant networks (DTNs).

Experiment Guidelines (For Bluetooth measurements)

There are three parts in this experiment: **Part I** is a preliminary data collection stage for Bluetooth device encounter traces. Each team is given a Bluetooth-enabled PDA with a program to detect and log encounters with other Bluetooth-enabled devices. The objective of this stage is to collect trace data in order to analyze and use it in the latter parts of the experiment. It also gives you the hands on experience and knowledge of trace data collection. Teams are suggested to work on possible scenarios of traces collection that have some regularity patterns.

Part II is the post processing and analyzing of the encounter trace. Teams will provide their understanding about Bluetooth encounters patterns. Parse the trace you downloaded from the website depending on your analysis. You can use your own database, excel or programmed parser. Possible questions to answers include number of encounters, distribution and regularity patterns in Bluetooth encounter, time duration of encounters etc.

Part III is optional. It is a comparison analysis of the encounter traces generated and another already generated encounter trace from the CRAWDAD website. The objective of this stage is to compare the different encounter traces generated in different time and place and see which characteristic hold similar and which characteristics do not.

Experiment Guidelines (For WiFi measurements)

There are three parts in this experiment: **Part I** is a preliminary data collection stage for (a) WiFi device encounter traces (via sniffing); and (b) APs syslog traces during the activity (a). Each team is

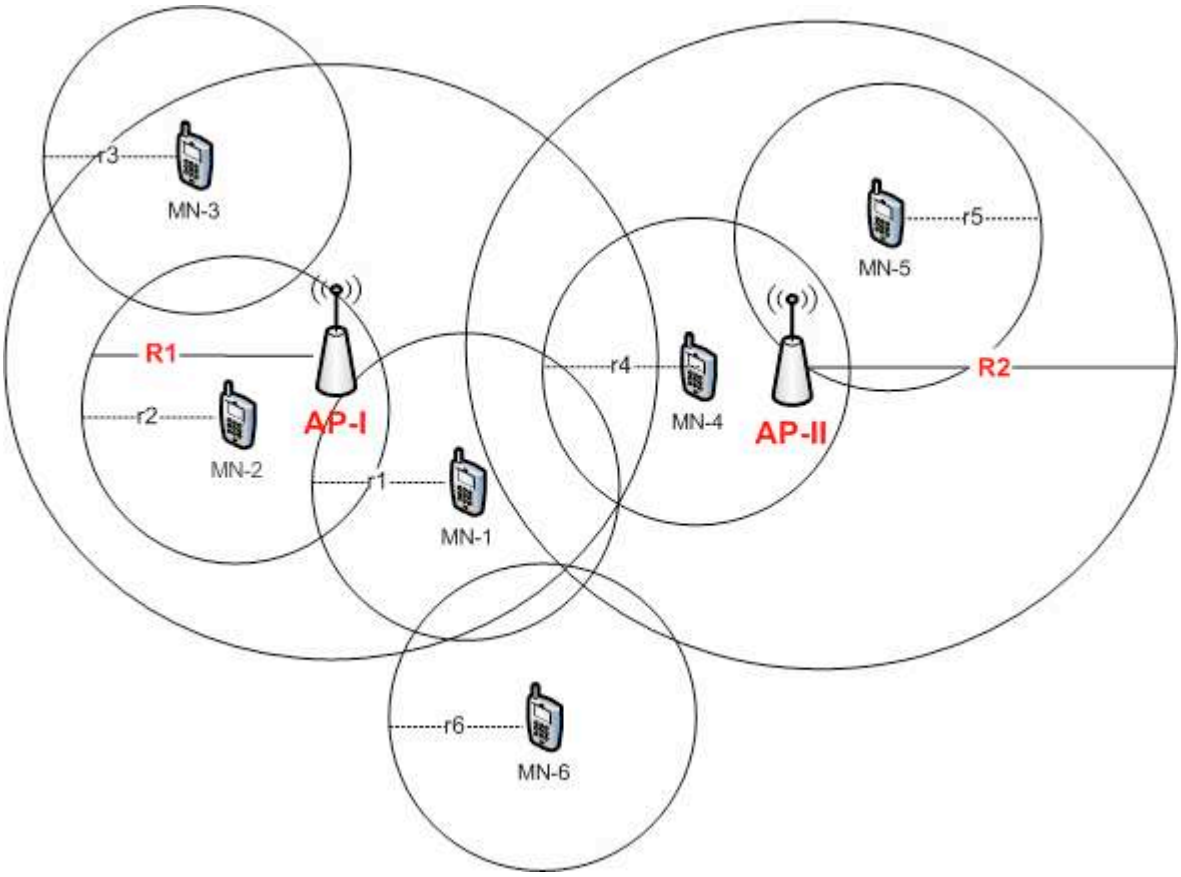

Figure 1: The figure has two APs, AP-I & AP-II with R1 & R2 radius respectively. There are total six MNs, MN-1 to MN-5 with radius r1 to r5 respectively, spread across the vicinity of APs. MN-1,2,3 belong to AP-I. MN-1, 2 can talk to each other directly. MN-4,5 belong to AP-II. They can talk to each other and MN-4 can also talk to MN-1 of AP-I. MN-6 with radius r6, is outside the range of both APs. But can talk to MN-1 of AP-1.

given a pair of two laptops or two network cards with a program to sniff and log encounters with other WiFi-enabled devices. The objective of this stage is to collect trace data in order to analyze and use it in the latter parts of the experiment. It also gives the hands on experience and knowledge of trace data collection methods. During this activity, teams will design a systematic method to sweep surrounding areas for other active MNs and also collect connected APs location traces.

In **Part II** of the experiment, team will process these traces and investigate the possibility of true encounters when:

1. MNs logged in to the same AP can communicate.
2. MNs logged in to the same AP cannot communicate.
3. MNs logged in to different APs can communicate, and;
4. MNs logged in to different APs and cannot communicate.

As shown in Figure-1, is one possible scenario of six MNs spread across two APs communicating with each other. This experiment is open ended and teams are free to add more possible scenarios. Optionally, the usage pattern of the devices, individual and group usage patterns, distance across APs, temporal barriers etc.

Part III of this experiment is to validate the above possibilities and provide their own analysis. Teams are required to validate the aforementioned assumption of "encounters" and provide a report of their understanding and investigation.

Notes

1. For WiFi experiment, collect traces from around six access points and number of measurements at every access point (around 30).

Optional Dimensions of Analysis

Teams can also identify the similarities and differences from the different environments presented by the traces and the potential applications of the findings on user modeling and protocol design. They can also provide best case, average case and worst case scenarios for actual encounters and their distribution. Adding to these investigation, teams can also provide a probabilistic model based upon valid statistical inferences that corroborate the assumption of encounters where communication between devices can actually be possible.

You can also think of the encounter as having a bandwidth (as opposed to either encounter '1', or no-encounter '0'), and "optionally" may make the measurements to reflect the bandwidth available between devices.

Teams can further extend these experiments to develop Models of information exchange in Bluetooth and WiFi networks. You can potentially correlate aggregate encounter patterns with specified properties of those encounters. And provide some insight on the similarity and differences in collected trace patterns and encounters for Bluetooth and WiFi networks.

Instruction to configure Nokias

Installing Kismet on Nokias 810.

Kismet (http://www.kismetwireless.net/)is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

1. For fast gps access install agps-ui from maemo extras. (or go to this link (http://betalabs.nokia.com/betas/view/gps-beta-nokia-n810) then click download and install and follow the instructions on the web site.)
2. Add the maemo chinook repository by clicking on this link. or going to (http://www.gronmayer.com/it/index.php?$lang = en\&system = maemo4$)
3. Activate RedPillMode in Application Manager, this allows you to see system libraries (open the Application Manager (application $->$ settings) then click on the top left corner of the application manager to get a menu. Choose tools$->$Application catalog. Click on New button. In the Web address field type in "Matrix" and then click cancel. This would show you a dialog box choose the Red Pill !!)
   - install libraries: ncurses-base and tcpdump
   - install rootsh

   (if you cannot install ncurses-base and tcpdump using the application manager but have installed rootsh. open the X-terminal $->$ become root by typing in root $->$ apt-get install ncurses-base tcpdump. close the application manager before you use apt-get)
4. Install deb build of kismet from TZ1 (http://www.zdez.org/nokismet-0.0.1a.deb). (click on the link to begin the installation)
5. For the gps access keep the map application running in background (application$->$My selection$->$Map).
6. in an xterm, do:
   - root
   - mkdir /media/mmc1/kismet
   - kismet
7. Note if you are not having an external memory card mkdir /media/mmc1/kismet would fail. Instead use $ mkdir /media/mmc2/kismet and as root edit the kismet.conf and change the location of the logs to mmc1 instead of mmc2. kismet.conf is located in /usr/etc/

For Scanning Bluetooth devices:

1. Download scanner.h file. (http://nile.cise.ufl.edu/wb/media/ukumar/scanner.sh)
2. This program allows us to scan bluetooth devices. It dumps the output in EncounterTrace.txt file.
3. Download this file on the internal memory card.
4. Open X terminal from utilities
5. $ cp /media/mmc1/scanner.sh ./
   $ chmod +x scanner.sh
6. Run the script by $./scanner.sh

7. You can change the interval between the consecutive scans by changing the parameter in the sleep command inside the script. 30 sec is generally too fast.
8. For taking out the EncounterTrace.txt, copy the EncounterTrace.txt to internal memory card and then attach it to emails.
   $ cp EncounterTrace.txt /media/mmc2/