CIS6930/4930 Mobile Networking - Spring 2012

Experiment 2

Due Date: 17 April 2012 (full credit)

TAs: Udayan Kumar (ukumar@cise.ufl.edu) - Saeed Moghaddam (saeed@cise.ufl.edu)

1) Introduction

In Experiment 1, you have been carrying a mobile device and collecting Bluetooth and AP traces. Experiment 2 will use these traces and look into several p2p applications. Experiment 2 is divided into two parts. In the first part of this experiment you will be analyzing the traces collected by you and other students in the class. In the second part, you will be asked to run several existing applications on your devices. The goal of this experiment is to give you insight into the information available in the traces, to get you started with trace analysis, which you would need for your projects, and to provide you with sufficient building (code) blocks so that you can start implementing your own applications on mobile devices.

In the optional section, you are free to perform any analysis you may find interesting. This would count towards extra credit. You are encouraged to think beyond the stated questions and perform analysis which may help you in understanding the mobile users or in collecting relevant data for your project.

** Please continue to collect and upload the traces as Experiment-1 will go on until 4/24 **

If you have any questions, please email TAs, Udayan Kumar (ukumar@cise.ufl.edu) or Saeed Moghaddam (saeed@cise.ufl.edu) or meet them during the office hours.

2) Trace Analysis

In this section you would analyze the traces belonging to your device and to the other students in the class. If you did not collect the traces please use the traces belonging to device N810-9/N810-12.

Traces can be downloaded from: http://www.cise.ufl.edu/~ukumar/traces-10-april-2012.zip

You can also access older traces from last spring using this link (format is different)
http://www.cise.ufl.edu/~ukumar/Latest-Traces-till-cis6930-sp11.zip

Important: The trace analysis for the most part is open-ended, meaning there is no one correct answer. A correct answer is the one that is supported by strong reasoning and analysis. So when answering the following questions, state your reasoning and assumptions clearly:

For the following analysis you (may) have to:

1. Write a parser to convert the raw traces into a format suitable for analysis. (you can collaboratively develop parsers with other students in the class)
2. Provide
   (a) Data table
   (b) Graph plot with proper labeling.
   (c) Explanation with proper reasoning of the results.

Questions

1. Compare and contrast the traces based on the following questions. Use all the traces collected by your group and at least 3 traces collected by other groups. Mention commonalities and differences and whenever possible provide a reason. (Use of graphs is highly recommended)

   (a) Write a brief description of the process you followed to collect the measurements. Did you

maintain a manual log of the measurement? What were the challenges during the measurement phase?

(b) What is the total number of encounters?

(c) What is the total number of unique encounters? (each Bluetooth MAC address counts as a single encounter no matter how many times they have met)

(d) Plot the graph of number of encounters per day for the whole length of the trace. Is there a pattern?

(e) Plot the graph of number of encounters per device. Is there a pattern ?

(f) Plot the access points (AP) and the number of times they appear in the traces. (top 20)

(g) Plot APs with corresponding number of bluetooth encounters (top 20). Is there a correlation between location and encounters?

(h) Can you identify from the traces if you were moving or stationary? Plot your movement patterns with respect to time.

(i) At what time (morning, evening, afternoon, night) do you have least Bluetooth encounters? Plot for all and provide an analysis.

(j) How many of the encountered devices belong to your friends? How many of them are added in your social network sites (Facebook, LinkedIn, Twitter, Google+, Orkut or MySpace, etc.) ?

(k) Identify at least three metrics that can be used to identify top encountering users (e.g., frequency of encounter can be one of the metrics). Using at least three of such metrics, identify top 10 users for each of the metrics.

(l) Rank all the MAC addresses of the devices encountered in the order of trust you have for the device owners. Please state the criteria you used for trust.

2. (Optional : Extra points)

Come up with interesting questions and analyze the traces to get the insight into user behavior (e.g. how many times did you encounter students from the class outside the classroom and at which locations, etc.).

You can also analyze traces coming from other sources and compare with your traces. Some of the other sources are :

(a) For traces imote-trace1/2/3, see descriptions at
http://crawdad.cs.dartmouth.edu/meta.php?name=cambridge/haggle

(b) For the reality mining trace see
http://crawdad.cs.dartmouth.edu/meta.php?name=mit/reality

(c) For the Singapore University trace (anonymized BT log) see
http://crawdad.cs.dartmouth.edu/meta.php?name=nus/bluetooth

(d) Another imote-trace is the trace collected in the city-wide experiment in Cambridge (imote-trace-cambridge), see http://crawdad.cs.dartmouth.edu/meta.php?name=upmc/content

3) iTrust

In this part of the experiment you have to evaluate the iTrust filters and the trust ratings received. You can generate the scores for each filter using the provided parser and scoring program.

1. Brainstorm of metrics (ways to measure) the success/failure of iTrust in generating trust recommendations. Come up with atleast 2 metrics and evaluate iTrust for all the traces using these metrics. An example metric can be the number of trusted users in top 10, top 20, etc recommendations by each filter.

2. Propose a new filter (one that is not available in iTrust), implement it and evaluate it using the metrics proposed in Question 1. (You can borrow code from existing parser and scoring program).

4) SUBMISSIONS

Write a full report on the analysis above and all of your other findings. Send the file (in PDF) of your report to the TAs before the deadline. Do not forget to mention the names of the students with whom you collaborated for either parser design or bluetooth experiment.

Deadline: 4/17 (full credit), 4/19 (90% credit), 4/24 (70% credit)

REFERENCES

[1] Weijen Hsu, Debojyoti Dutta, and Ahmed Helmy, "Profile-cast: Behavior-aware mobile networking", In Proceedings of IEEE WCNC, March 2008.

[2] Weijen Hsu, Debojyoti Dutta, and Ahmed Helmy, "CSI: A paradigm for behavior-oriented profile-cast services in mobile networks", Adhoc Networks Journal – Elsevier, In press.