CIS6930/4930 Mobile Networking - Spring 2012

Experiment 1

Final Due Date: April 19, 2012 - (weekly traces submissions and iTrust submission on March 1, 2012)

Start Date: February 20, 2012

1 Introduction

This experiment will allow you to collect Bluetooth and Wi-Fi AP traces. In this experiment, these traces will be used to run iTrust application. Later these traces will be used in other experiments for this class and can be used by you for your projects.

Bluetooth trace is produced by the result of scanning all the visible Bluetooth devices; the Wi-Fi AP trace is produced by result of scanning all the visible Access Points. Bluetooth trace can give insights into encounter patterns and AP trace can be clubbed to get location information. We support Android and Nokia N800/N810 devices for this experiment. Both the devices produce one file each for Bluetooth and Wifi scanning. The format is slightly different between the Android and Nokia devices.

Please carry the device with you and run the scripts/Application for as long as possible every day to get complete traces.

2 General Instructions

1. Do not exchange devices with anyone, this will insure that all the traces belong to your movement.
2. Check the battery indicators frequently and keep the devices charged up. A dead device also means loss of traces.
3. Periodically take a backup of the traces using any method suitable for your device.
4. You are also encouraged to keep a log of all the locations you visit, while carrying the device, this would give you a better sense of location, when doing the analysis.

3 Devices

Currently, we have about 12 Nokia Devices (N810 and N800) available for the checkout, we request students who own android phone to run iTrust app on their devices for scanning.

Below are the usage guides to Nokia and Android devices.

4 Nokia N810/N800

Configuring Nokia's N810 to collect Bluetooth and WiFi Traces (http://maemo.org/).

4.1 Preliminary Settings & Checks

1. Boot the device using Power button on the top.
2. Click on the WiFi signal icon on the top right corner, adjacent to battery. Then click "Connectivity Settings", then click "Idle times" tab. Make sure "WLAN idle time" is select to "Unlimited". If not, select it from drop down menu and press ok.

3. Check “iwlist” is present. To check - click on the program menu ->utilities ->X Terminal. Run following commands
   - $ root
   - $ iwlist
   If it gives “command not found”, take the device to TA in the office hours.

4. Enable Bluetooth. Click “Settings” - >“Control Panel” - >“Bluetooth”. Make sure “Bluetooth On” & “Visible” is checked and device name is present (do not change the name, later it will help you to identify devices in the analysis).

4.2 Register Device

Please register the bluetooth address of your Nokia device on the following website : http://128.227.176.22:8182/. This will allow other students in the class to find out who they encountered with. The lookup can be performed here : http://128.227.176.22:8182/getData.html. The lookups can also be done form inside ‘itrust’ application when Nokia device is connected to Internet. To find the MAC address, take out the battery and ruse BT mac (please make sure to put colons after each pair of digits).

4.3 Trace Collection Process

1. For trace collection, open the “X Terminal”. Enter “root” followed by “ls -lt” command and make sure scanner.sh file is present with executable permissions.

2. Run the script (./scanner.sh) to start trace collection process.

3. To stop it, press ctrl-c.

4.4 Transfer the file to laptop/desktop

1. The files named “EncounterTrace.txt” and “wifi-data.txt” are generated at /media/mmc2 location. To download it, connect your N810 to windows/linux machines. Browse the file in the /media/mmc2 location and copy to a desired folder.

2. You can also get it by **email attachment** via web-browser (by connecting the device to a wireless network).

4.5 iTrust

In this experiment you have to use the application *itrust* and answer the questions stated in the following section. The application is already present in all the devices in the /root directory. If it is missing it can be downloaded from here :

http://dl.dropbox.com/u/967042/itrust or http://goo.gl/TNZ6a

(currently the application only works on Nokia devices)

This application should be used when one has collected atleast one week of data. In case on any questions regarding ‘iTrust’ please contact Udayan Kumar (ukumar@cise.ufl.edu)

4.5.1 Usage Instructions

The application can be started by :

```
./itrust <bluetooth-trace> <wifi-trace>
```

Typically the bluetooth trace is located here : /media/mmc2/Encounter-Trace-N810.txt Typically the wifi trace is located here : /media/mmc2/wifi-data.txt

Note1: if you have split your scanner files. Combine them together maintaining the temporal order then use the combined file as the input to itrust.

Note2: please stop the scanning process while you are running this application.

Note3: if you get segmentation fault while generating recommendations, check that scanner is not running and reboot the device, then try again.

4.5.2 iTrust Deliverables

- Please report the general stats from option 1 of the application.
- Check recommendations provided by four filters, one at a time. Add the users you can trust to the trust list. You can find more information about the devices/users by going into details menu. (By trusting a user, we mean, you would be ready to route messages for that user). Once you add a user to trust list, that user will not be shown again. Therefore, after using each filter you have to delete the file .iTrust_ trusted_mac. This file stores all the trusted macs and a mac once trusted will not be recommended again.
- Use the combined filter. Add the users you think can be trusted. Is combined filter proving better recommendation? (delete the .iTrust_trusted_mac file before starting)
- Please mention any surprise you could got from the application in term of recommendation.
- Try adjusting the combination ratio in combined filter. Do you find better recommendations at some ratio? please mention the ratio
- More points will be awarded to students showing high usage activity. High activity does not imply marking every user as trusted :).
- For the submission send a report answering the questions above and a file named 'log-trust'. This file should be present in the same directory as application 'itrust'. (you may have to copy log-trust to the internal memory card /media/mmc2/, before sending it over email to Udayan Kumar (ukumar@cise.ufl.edu)

5 Android

On android devices, the scanner for wifi and bluetooth is integrated with iTrust application. The application can be downloaded from here :

http://128.227.176.22:8182/iTrust.html please enable installing of application from unknown sources (generally in settings− >Application)

5.1 Starting the scanner

Go to the menu − > Start Scanning. The files are create in the sdcard in the 'iTrust' folder. The raw traces are stored in files 'scannedData*' and once they are processed they are appended to 'ZIPscannedData*'

5.2 updating encounter scores

Once you have started the scanner, you can refresh the score to get latest encounter scores. You can also update the locations information using 'Update Locations' menus option (This requires Internet connection).

5.3 Register Device

One can register the device from within the application (Menu − > Register). Please register your device. This will allow other students in the class to find out who they encountered with. The lookups can be performed from with the application by clicking on the MAC address (blue color font) from the user's detail encounter page. The lookup can be performed here : http://128.227.176.22:8182/getData.html. Lookups require Internet access.

5.4 Sending files

Files can be send by using the 'Upload Encounter' option from the menu. Only 'ZIPscannedData*' and 'ClickDataLog' files will be uploaded. Please **refresh scores** before uploading encounters.

5.5 Deliverables

- Add the users you can trust to the trust list. (By trusting a user, we mean, you would be ready to route messages for that user). You can find more information about the devices/users by clicking on the MAC address/Device Name. You can add devices to trust list (both high trust and no trust options can be selected)
- you can sort users by different filter. Please note the filter that gives you most relevant results.
- Set weight option allows one to change how filter results are combined together (make sure your sorting key is set to combined score). Is combined filter proving better recommendation? Try adjusting the combination ratio in combined filter. Do you find better recommendations at some ratio? please mention the ratio
- Please mention any surprise you could got from the application in term of recommendation.
- More points will be awarded to students showing high usage activity. High activity does not imply marking every user as trusted :).
- For the submission send a report answering the above questions to Udayan Kumar (ukumar@cise.ufl.edu).

6 Evaluations and Deadline

Evaluations are based on two components : 1. number of days worth of traces collected and 2. the activity shown in the iTrust logs based on the deliverables mentioned in the sections above.

Trace collection can continue till April 19, 2012. However, traces should be submitted weekly. Deadline for iTrust deliverables is **March 1, 2012**.

For Android devices, weekly (more is better) upload encounters and for Nokia devices, send traces and iTrust log file to Udayan Kumar on weekly intervals.