CIS6930/4930 Mobile Networking - Spring 2013

Experiment 1

Instructor: Ahmed Helmy, Teaching Assistant: Guliz Tuncay, Original Assistant: Udayan Kumar

Start Date: February 18, 2013

- Weekly traces submissions and iTrust deliverables submission on March 1, 2013.
- One report per group should be submitted [check the 'Deliverables' section below].
- Traces to be submitted individually.
[the iTrust app can automatically submit your traces]
- Final Due Date for all (semester long) traces: April 23, 2013.

1 Introduction

This experiment will allow you to collect Bluetooth and Wi-Fi Access Point (AP) traces. In this experiment, the *iTrust* application will be used to collect these traces. In a later experiment, these traces will be used in other experiments for this class and can be used by you for your projects. So, you are expected to continue to collect traces using *iTrust* for the whole semester.

The Bluetooth trace is produced by scanning all the visible Bluetooth devices, and the Wi-Fi AP trace is produced by scanning all the visible Access Points. The Bluetooth trace can give insights into encounter patterns and AP trace can be used to get location information. We support Android and Nokia N800/N810 devices for this experiment. Both the devices produce two files; one for Bluetooth scanning and another for 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 more complete traces.

2 General Instructions

1. Try not to 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. 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 performing the analysis.

3 Devices

It is best if you can download and run the Android app on your device (if you have one). Otherwise you can check out a Nokia device from the lab (please contact the TA to setup a time for device check out). Currently, we have about 12 Nokia Devices (N810 and N800) available for the checkout.

Below are the usage guides to Nokia and Android devices.

4 Android

On android devices, the scanner for wifi and bluetooth is integrated with the *iTrust* application. The iTrust (originally developed by Udayan Kumar during his Ph.D. at UF) has been released under open source license. The latest version of iTrust and its code can be downloaded from the following link: https://code.google.com/p/itrust-uf/

Please enable installing of application from unknown sources (generally under Settings− >Application)

For more information please press the 'menu' option from the app itself after installation, press 'more' and press 'Help'. For even more information, you can visit: http://128.227.176.22:8182/iTrust.html

4.1 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*' (scannedDataB for Bluetooth traces and scannedDataW for WiFi traces). Once these files are processed they are appended to 'ZIPscannedData*'.

It may take you a few minutes to start seeing any device listing, and you may have to go next to discoverable bluetooth devices to see more entries.

Scanning in general takes some resources and battery power. You can also use the 'energy efficient scanner' under menu − > more − > Settings to save power. [More info about the energy efficient scanner is available in the paper by U. Kumar, A. Helmy in the ACM SenSys PhoneSense workshop 2012.]

If you want other devices (e.g., your classmates or project group members) to be able to discover your device, you may have to turn on the discoverability of your Bluetooth (under Settings − > Wireless & Networks). If your device is running Android 4.0 (Ice Cream Sandwich 'ICS' or above) iTrust may set the discoverability of your device indefinitely [you may be prompted to approve this setting once in the beginning of the iTrust operation]. This may cause your battery to drain a bit faster, so please keep your device charged.

4.2 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). [Note: one some devices the update location option may force a close of the application. If that happens restart the app and continue using it, as this would not affect its trace-collection capabilities.]

4.3 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. The registration information is kept (in encrypted form) on a server in our lab.

4.4 Sending files and uploading traces

As part of this assignment you are required to upload your traces weekly. The latest iTrust release on Android automatically uploads the traces for you, so you do not have to worry about it. You can double check the 'Upload Traces periodically' option under 'menu − > more − > Settings' in the app.

[Note: If you 'uncheck' that option (we recommend that you leave that option 'checked', but just in case you do uncheck it) then you would have to upload the traces manually. Files can be sent by using the 'Upload Encounter' option from the menu. Only 'ZIPscannedData*' and 'ClickDataLog' files will be uploaded. Please **refresh scores** before uploading encounters.]

4.5 Deliverables

- Click the devices and slide the trust score: 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 the devices/users using different filters [choose menu $->$ sort]. Please note the filter that gives you most relevant or useful results. There is a frequency of encounters (FE) filter, duration of encounters (DE), a location vector count (LV-C), and location vector duration (LV-D) score filters. For more information about filters please read the related papers by U. Kumar and A. Helmy, et al. The combined filter is explained below.
- The combined filter integrates different scores from all four filters. The 'Set weights' option [menu $->$ image of a person lifting weights] allows one to change how the filter results are combined together (make sure your sorting key is set to combined score). Is the combined filter providing better recommendations? Try adjusting the combination ratio in the combined filter by adjusting the weights. 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 Guliz Tuncay (gstuncay@cise.ufl.edu).
- **Each group will send only one report.**

5 Nokia N810/N800

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

5.1 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).

5.2 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).

5.3 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.

5.4 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).

5.5 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) or Guliz Tuncay (gstuncay@cise.ufl.edu)

5.5.1 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.

5.5.2 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 Guliz Tuncay (gstuncay@cise.ufl.edu)
- **Each group will send only one report.**

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, 2013**.

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