The analysis of passive Wi-Fi tracking

Wouter Bakker, University of Twente, Faculty EEMCS

***Abstract*—Nowadays almost everyone has a smartphone. Smartphones are sending a lot of Wi-Fi packages. These packages are send even when they are not connected to a Wi-Fi network. With all the information that smartphones are sending, it should be possible to track and count all the phones and say something about the amount of people in an area.**

To get an inside in the Wi-Fi behavior of a smartphone, four different phones are analyzed. Every phone is tested in different circumstances. Since apps might change the behavior of a phone, additionally, different apps were tested in these circumstances as well to see if apps will increase the amount of Wi-Fi packages.

Not only have the tests been executed in a controlled environment, they have been accomplished in an uncontrolled environment as well. In a 3-hour measurement, more than 12.500 packages of unknown devices are captured and analyzed.

The results show interesting results, especially when it comes to iPhones. It seems that some iPhones are not always sending the real MAC-address of the phone when dispatching Wi-Fi packages. iPhones can send locally administered MAC-addresses. These addresses are random and switched over time. Thus one iPhone can send multiple MAC-addresses. A measurement has been performed to count this changing of addresses and get an insight in the frequency of changing. With this information, more knowledge has been gained over the amount of iPhones in an area.

This paper will show that is possible to track people by capturing all packages that their smartphone sends and how this is done.

***Index Terms*— Passive Wifi tracking, locally administered MAC-addresses**

I. Introduction

Passive Wi-Fi is not new; it is already being used by some marketing companies. These companies track smartphones and make personal marking campaigns. Moreover, festivals are using this technique to count the number of festival visitors. Although companies are using the principle of passive Wi-Fi already, there are a lot of unknowns when measuring the Wi-Fi packages that smartphones are sending.

Smartphones are sending a lot of different packages. What kind and how many packages a phones sends depends on the vendor and type of phone. In this paper a more thorough analysis of packages transmitted is performed. This includes the following sub questions:

- Should the sensor listen on one Wi-Fi channel or is hopping better?
- Which type of packages are different phones sending and what is the frequency of sending?
- What is the benefit of heaving multiple sensors close together?

The paper is structured as follows. The related work is in section 2. In section 3, the method of the research will be elaborated. The results can be found in section 4. The paper ends with a condusion and discussion section in section 5.

II. Related work

A. Tracking of human beings

To determine the amount of people in certain area with basic Wi-Fi hardware, different methods can be used. Most of these methods [1] [2] [3]contain tracking human beings instead of tracking their devices. To determine human beings, Doppler measurements can be used. [2] Another tracking method [3] is to make a radar fingerprint of an area. To get a radar fingerprint of an area, the signal strength information at multiple base stations will be measured. When a person moves, the signal strength information is changing over time. [3]

B. Tracking of smartphones

Tracking human beings has become relatively easy since most human beings own a smartphone. [4] So instead of tracking human beings, it is possible track their phones. A smartphone periodically transmits Wi-Fi packages. When a smartphone is sending a Wi-Fi package, it also sends its MAC-address. These MAC-addresses are unique per devices and can therefore be used to track and count smartphones. [5]

C. Different Antennas

An antenna with a relatively big gain will capture more wireless devices then an antenna with a relatively small gain. [6] The dataset of a small gain antenna has been optimized compared to the dataset of a big gain antenna. However, a high gain antenna has better performance when a wireless device is moving fast. [6] Since there was no opportunity to measure devices with different antennas, the measurements in this paper will be conducted with one sensor and a single antenna.

III. METHOD

A. Distribution of channels and package types in a controlled environment

The 2,4 GHz Wi-Fi band has thirteen different channels in Europe. Every Wi-Fi package has a package type and a package subtype. To be able to distinguish which package was send on which channel, a test setup was created. The test setup contains a Wi-Fi sensor and 4 smartphones. The sensor captures all the packages and sends them to a MySQL database. The Wi-Fi sensor is a Bluemark 510. To see if there is a big difference between different type of phones, this test includes multiple phones. The tested phones are:

- Apple iPhone 4s running IOS 9.3.2
- Apple iPhone 5s running IOS 9.3.2
- Sony Xperia U running Android 5.1.1
- General Mobile – Android one running Android 6.0.1

All phones have been reset to factory default prior to the test to get a good baseline measurement. A list of 5 Wi-Fi networks is saved to every phone. To get a good insight in the send Wi-Fi packages, all the phones are tested in different circumstances.

First test:
The phones are laying on a table. No extra apps are installed and the screen is turned off. None of the saved Wi-Fi networks are in range of the phone.

Second test:
The phones are laying on a table. No extra apps are installed. The screen is turned on. None of the saved Wi-Fi networks are in range of the phone.

Third test:
The phones are laying on a table. No extra apps are installed. The screen is turned off. All phones are now connected to a saved Wi-Fi network.

Fourth test:
The phones are laying on a table. Facebook is installed as extra app and a Facebook user is logged in. The screen is turned off. None of the saved Wi-Fi networks are in range of the phone.

Fifth test:
The phones are laying on a table. Skype is installed as extra app and a Skype user is logged in. The screen is turned off. None of the saved Wi-Fi networks are in range of the phone.

The Wi-Fi sensor captures all Wi-Fi packages for one hour and each test is repeated two times. This is to locate on which channel which type package is send. The sensor switches every second to one of the 13 channels. The channel is selected at random. From every received package the following information is saved. The package type, the package subtype, the RSSI, the channel, the time on which the package is received and the MAC-address from the sender.

After the measurement, the database contains all Wi-Fi packages from all Wi-Fi enabled devices in range of the sensor. Only the packages send from the tested phones are interesting, so all packages where the received MAC-address corresponds to the real MAC-address of the phone are stored in a separate database table and used for further analyses.

B. Distribution of channels and package types in an uncontrolled environment

In reality it is likely that the list of saved networks is typically much higher than the 5 in in controlled environment. Furthermore, it is likely that the smartphone users installed different types of apps on his smartphone. Or at least more apps than the single one in the controlled environment. Therefore, a test in an uncontrolled environment was performed.

For this test the same sensor was used as in the controlled environment. But now the sensor was battery powered and put in a backpack. This backpack was carried through the center of Enschede for a few hours. In contrast to the controlled situation, the sensor is not connected to the internet so data is buffered in the sensor. After the walk, the sensor is reconnected to the internet and all data is uploaded to the MySQL database. The sensor again switches every second to one of the 13 channels and the selected channel is selected at random. For every package the same information is saved as in the controlled experiment.

C. R used by IOS devices

Starting from IOS 8, Apple introduced random MAC-addresses [7]. When a phone is not connected to Wi-Fi network, it sends probe requests. Together with that probe request it also sends it MAC-address. When an iPhone running IOS 8 sends a probe request, it can send a random MAC-address instead of the real MAC-address of the phone. [7] To measure this random MAC-address, a small test setup was made. The iPhone 5s and the Bluemark 510 sensor were put in a box. To ensure the that the sensor only receives packages from the iPhone and not from other Wi-Fi enabled devices, two measurements are taken. First, the box has bene packed with tin foil. The foil ensures that the Wi-Fi signals from outside will be muted. Secondly, only the sensor has been put in the box to get an insight in the performance of the box. The only received signals for the sensor were the signals with a signal strength lower then -60dBm. When the iPhone is put in the box, the sensor received signals up to 27dBm. To capture only the packages, send by the iPhone, all signals below -60dBm will discard. Again, the sensor switches to one of the thirteen channels every second and the selected channel is selected at random. The Bluemark sensor can indicated if a received MAC-address is a locally administered addresses or is a universally administered addresses. This information is saved as well.

IV. RESULTS

A. Distribution of channels

When the tested smartphones are not connected to a Wi-Fi network they send Wi-Fi packages to all Wi-Fi channels. This Wi-Fi packages are equally distributed over all channels. See Figure 1 for the measurement results for the first test as described in the method section.

When the tested smartphones are connected to a Wi-Fi network the result is completely different. The smartphones almost exclusively send packages to the Wi-Fi channel of the connected access point. This result can be seen Figure 2, which is the result of the third test as descripted in the method. The connected channels in the first measurement are 5 and 13. The iPhone5s was in this case connected to the 5gHz version the of the network and the sensor was not able to capture packages on the 5 GHz band. In the second measurement the connected channels are 1 and 9.

B. Distribution of package types

The type of package a smartphone is sending is highly dependent on the Wi-Fi connectivity of the smartphone. When a smartphone is not connected to a Wi-Fi network it will only send probe requests, but when the smartphone is connected it will send all types of packets. In Figure 3 and in Figure 4 are the measurement results of test one.

The test in the uncontrolled environment confirms the found results in the controlled environment. According to Figure 7 all probe requests are equally distributed over all channels. The amount of null data packages is higher on the channels 1,6 and 11. Which can be explained. Access Point are sending bacon frames to announce their SSID. The amount of this beacon frames is much higher on the channels 1,6 and 11 so it is likely that much more smartphones are connected to these channels.

C. The impact of the screen

The state of the screen of the smartphones is an imported factor for the amount of packages a smartphone is sending. When the screen is on, test two, both android phones are sending much more packets then the in case when the screen is off. The iPhones4s has the exact opposite behavior. The results are in Figure 5. It seems that the Sony Xperia is not sending any packages when its screen is off.

D. The impact of apps

When Facebook or Skype is installed on an iPhone 4s an increase of Wi-Fi packages is measured. On the General Mobile phone, the amount of packets varies too much. So it is not possible the say something useful over that measurement. The results can be found in Figure 6.

E. Rate of sending packages

The time between two received packages depends highly on the type of smartphone, the energy state of the smartphone and the installed apps on the smartphone. The minimal rate of received probe requests was 9 request per hour and the maximum amount of probe requests was 513 per hour.

The maximum amount of received null data packages was 97 packages per hour.

F. The impact of more receivers

When the phone is not connected to a Wi-Fi network all packets were equally distributed over all Wi-Fi channels. When adding more Wi-Fi sensors, the change that you capture more packages will increase. When a sensor is fixed to one of the 13 Wi-Fi channels. The sensor will capture 1 out of the 13 packages. When adding exact the same extra sensor, but that sensor will listen to another channel. The sensors will capture 2 out of the 13 packages. So to get in theory a 100% change, you need 13 sensors. All sensors must have the range and must in the place.

The amount of phones that will detected depends on the time that smartphones are in range of the sensors. When a phones is a relative short time in range of the sensors it will send less packages therefor more sensors are needed to detect the smartphone.

When a smartphone is connected to a Wi-Fi network it sends most of this packages on the connected channel. To detect this phones, it is useful to detected that connected channel and set the sensor to that channel. The amount of sensors depends on the amount of channels that are in use by the access points nearby.

G. Locally administered MAC-addresses used by IOS devices

The tested iPhone 5s send all its probe requests with a locally administered MAC-address. That was the reason that in all other measurements no probe requests from the iPhone 5s were registered. The MAC-addresses are changing over time and the average period that MAC-address is the same is about 20 minutes.

V. CONCLUSION

In conclusion, this paper shows that is it possible to determine smartphones by using Wi-Fi monitor sensors. The chance that a smartphone is detected highly depend on the type of smartphone. Moreover, the amount of packages a smartphone sends depend on the user configuration of the smartphone.

Although the research takes many circumstances into account, it can be improved in next measurements. All phones used in the controlled experiment had no active sim card installed, so the phones were not connected to a mobile data network. There were only 5 Wi-Fi networks saved on the smartphone, it has not been tested if an increase of the saved networks will increase the amount of probe requests send by a smartphone.

The research was done with one sensors which was switching between all 13 Wi-Fi channels. So the sensor was able to capture only one channel at a time. A better measurement setup could use

13 sensors. With 13 sensors it is possible to capture all 13 channels at the same time. Furthermore, no Wi-Fi packages send on the 5gHz Wi-Fi band were captured. Relatively new phones will also send probe requests on this band.

The measurements on the random MAC-addresses can be done anew in a real Faraday cage to ensure that there is no interference from other Wi-Fi enabled devices.

VI. BIBLIOGRAPHY

[1] A. E. K. M. Y. Ahmed Saeed, "A Low-Overhead Robust WLAN Device-Free Passive Localization System," 2014.

[2] P. Falcone, "Localization and tracking of moving targets with WiFi-based passive radar," Rome, Italy, 2012.

[3] P. B. a. V. N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System," in *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (INFOCOM '00)*, 2000.

[4] GfK, "GfK," 2015. [Online]. Available: http://www.gfk.com/nl/insights/press-release/geen-groei-meer-in-bezit-mobiele-devices/.

[5] J. E. A.B.M. Musa, "Tracking Unmodified Smartphones Using Wi-Fi Monitors," Chicago, 2012.

[6] A. B. E. C. M. M. Naeim Abedi, "Assessment of antenna characteristic effects on pedestrian and cyclists travel-time estimation based on Bluetooth and WiFi MAC addresses," Australia, 2015.

[7] C. M. M. C. L. S. C. F. P. †.-D. Mathy Vanhoef†, "Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms," Lyon, France, 2016.

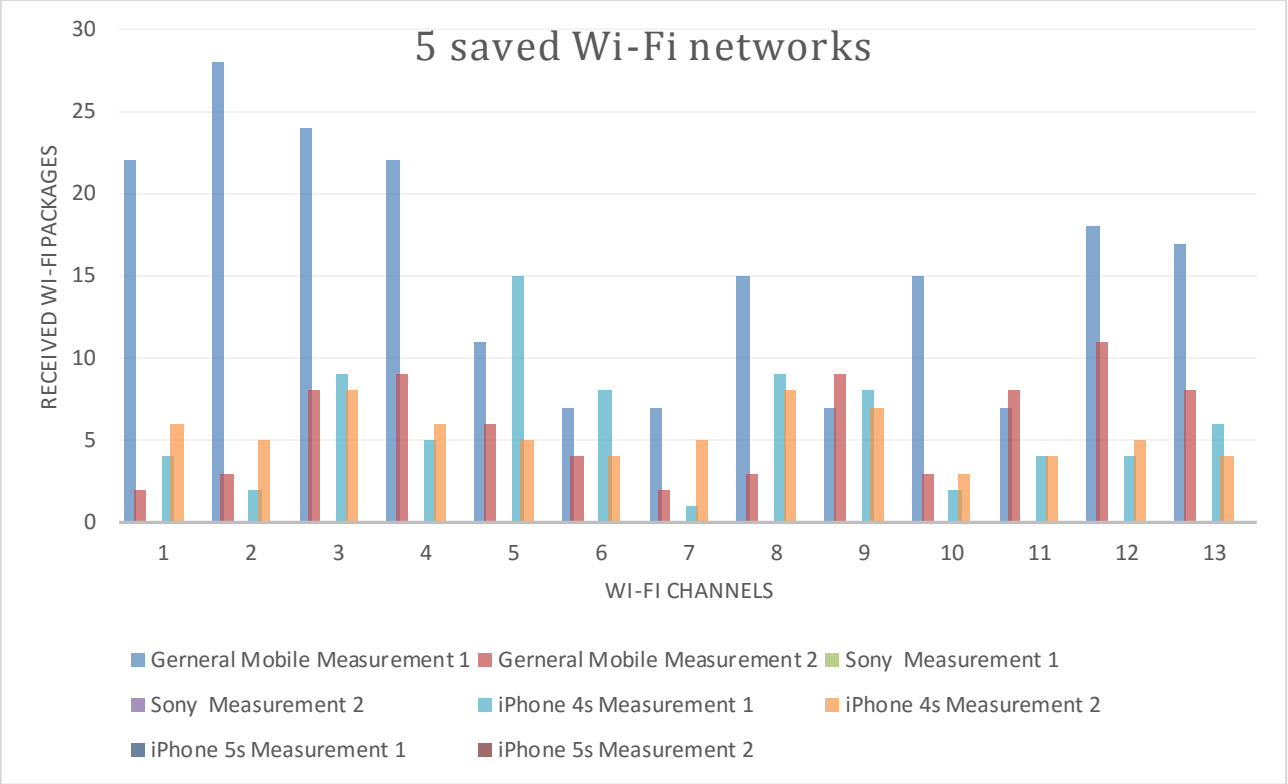

Figure 1: 5 saved networks

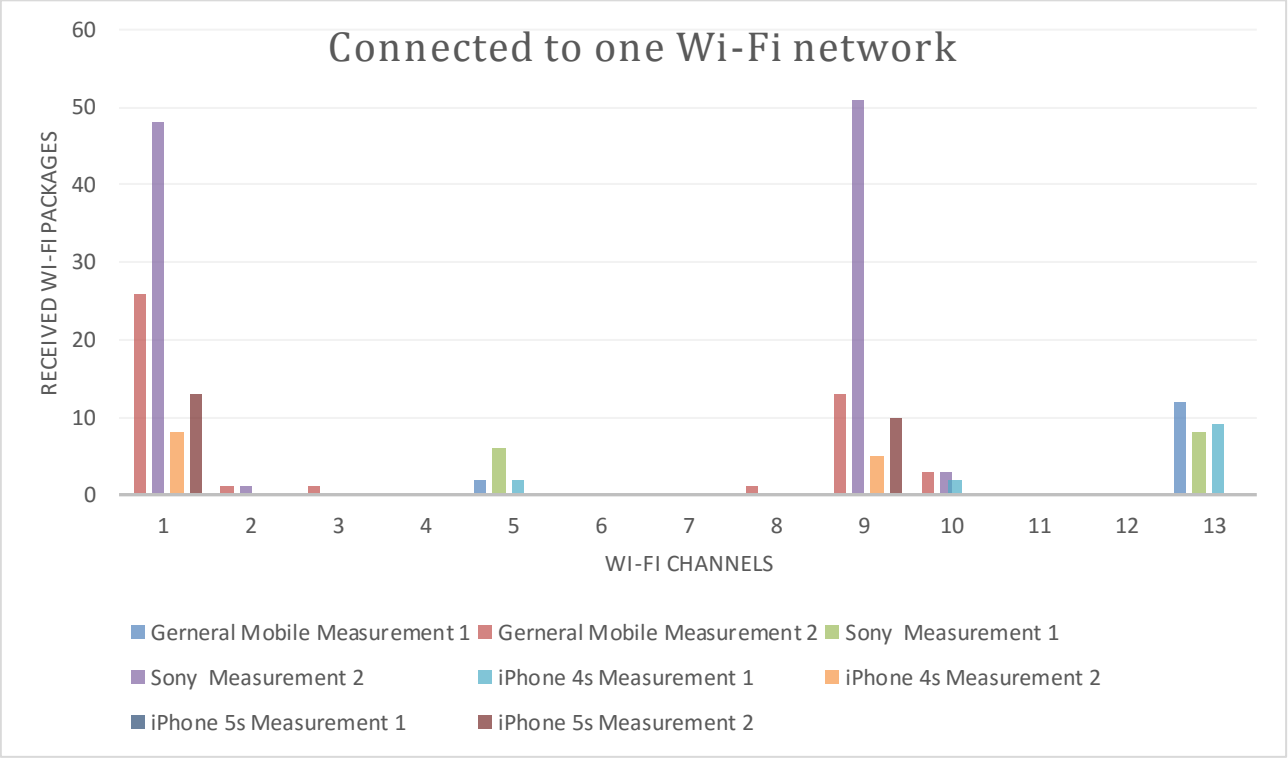

Figure 2: Connected to one Wi-Fi Network

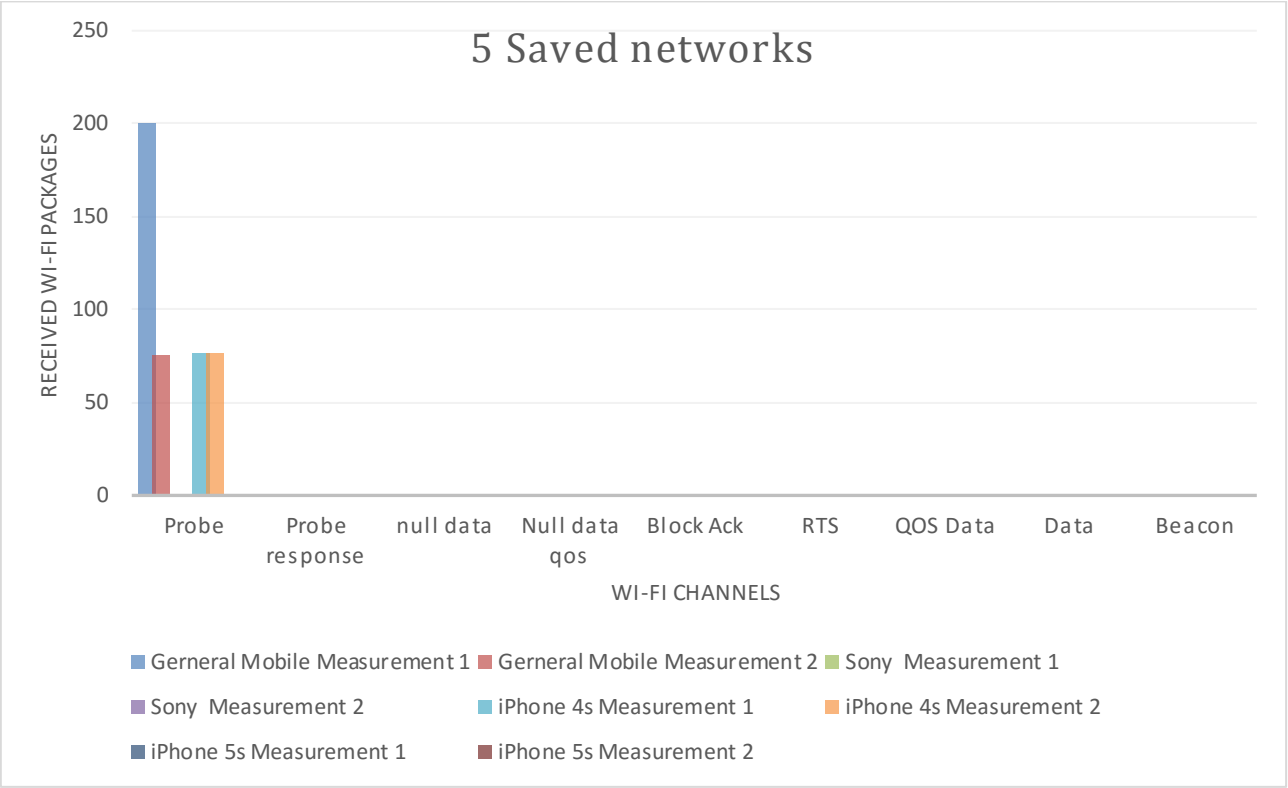

Figure 3: Package distribution, when a smartphone is not connected to a Wi-Fi network

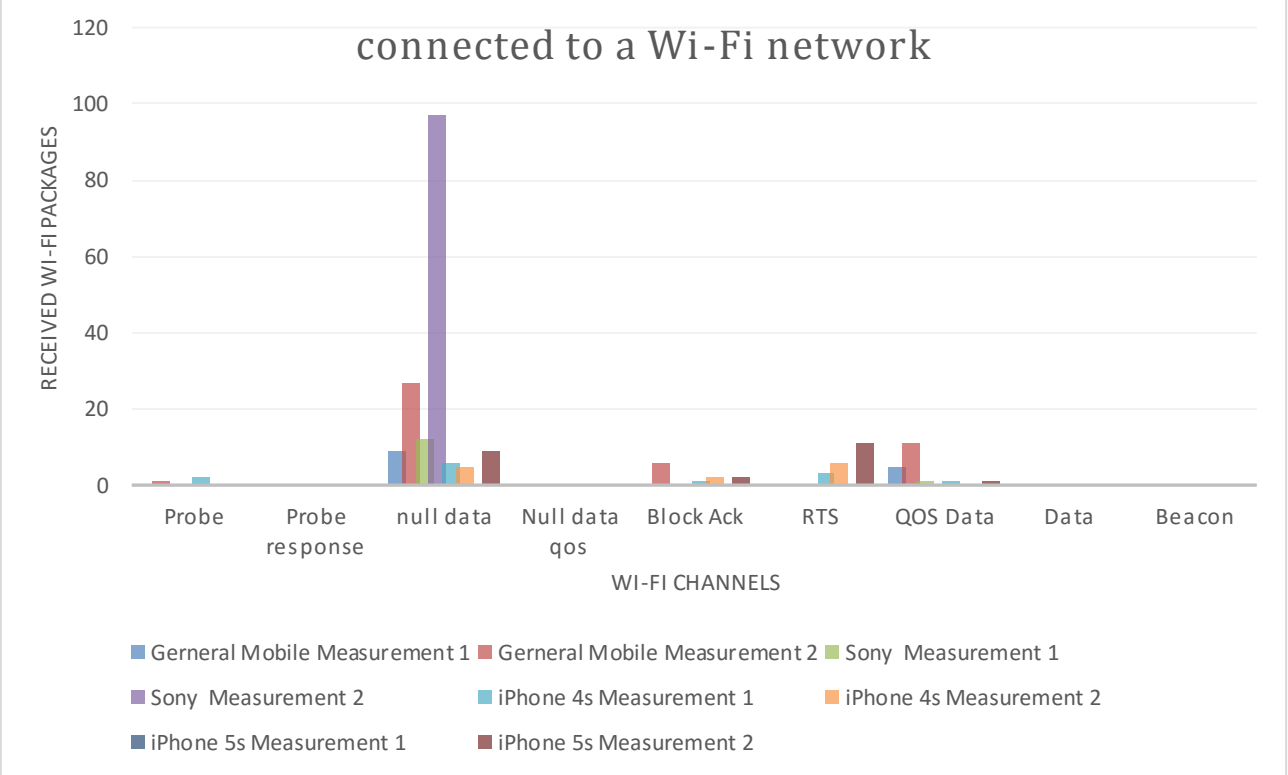

Figure 4: Package distribution when a smartphone is connected to a Wi-Fi network

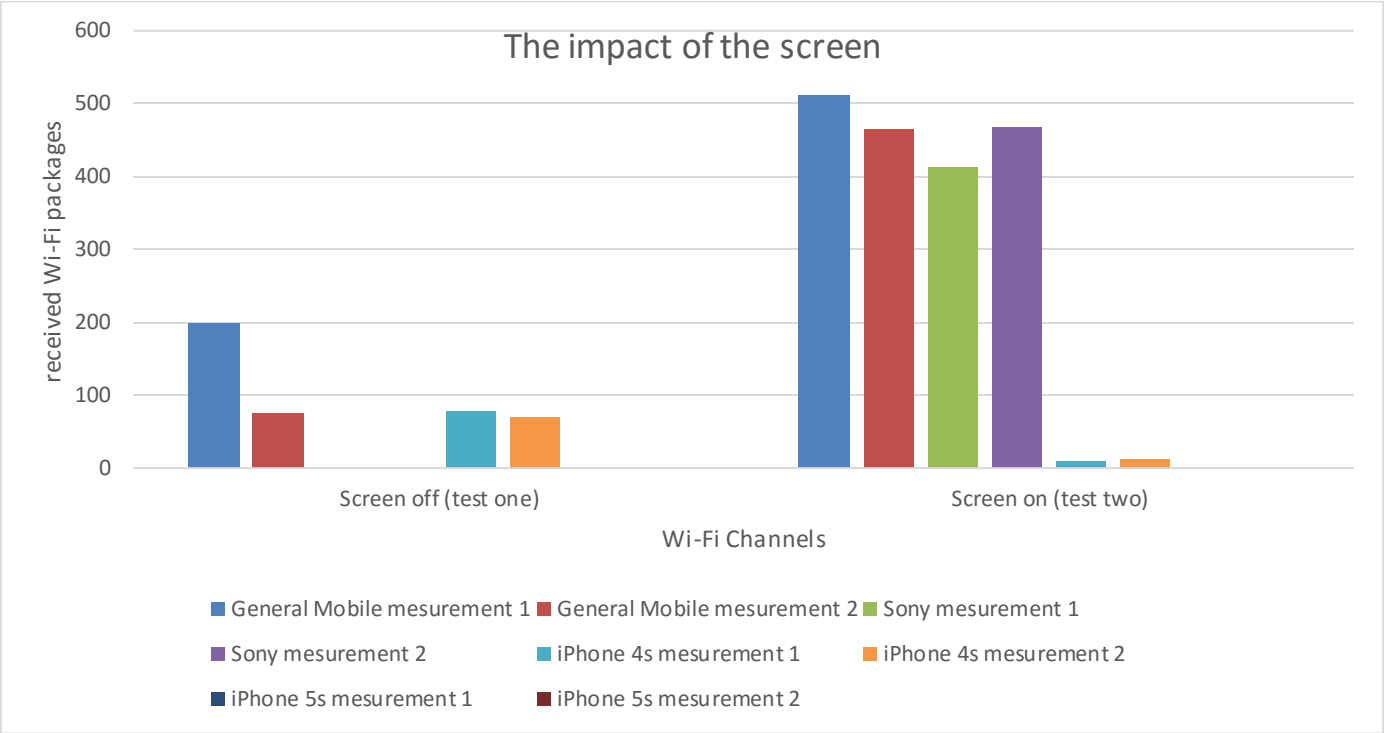

Figure 5: the impact of the screen

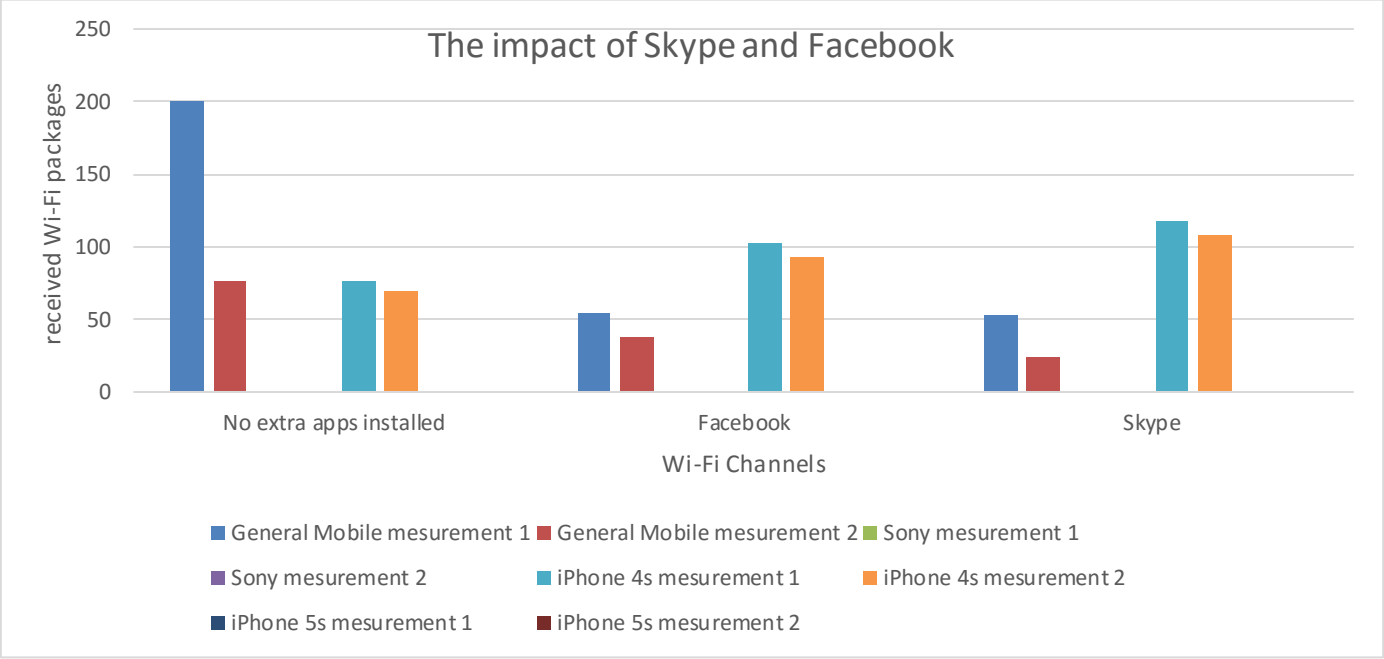

Figure 6: The impact of apps

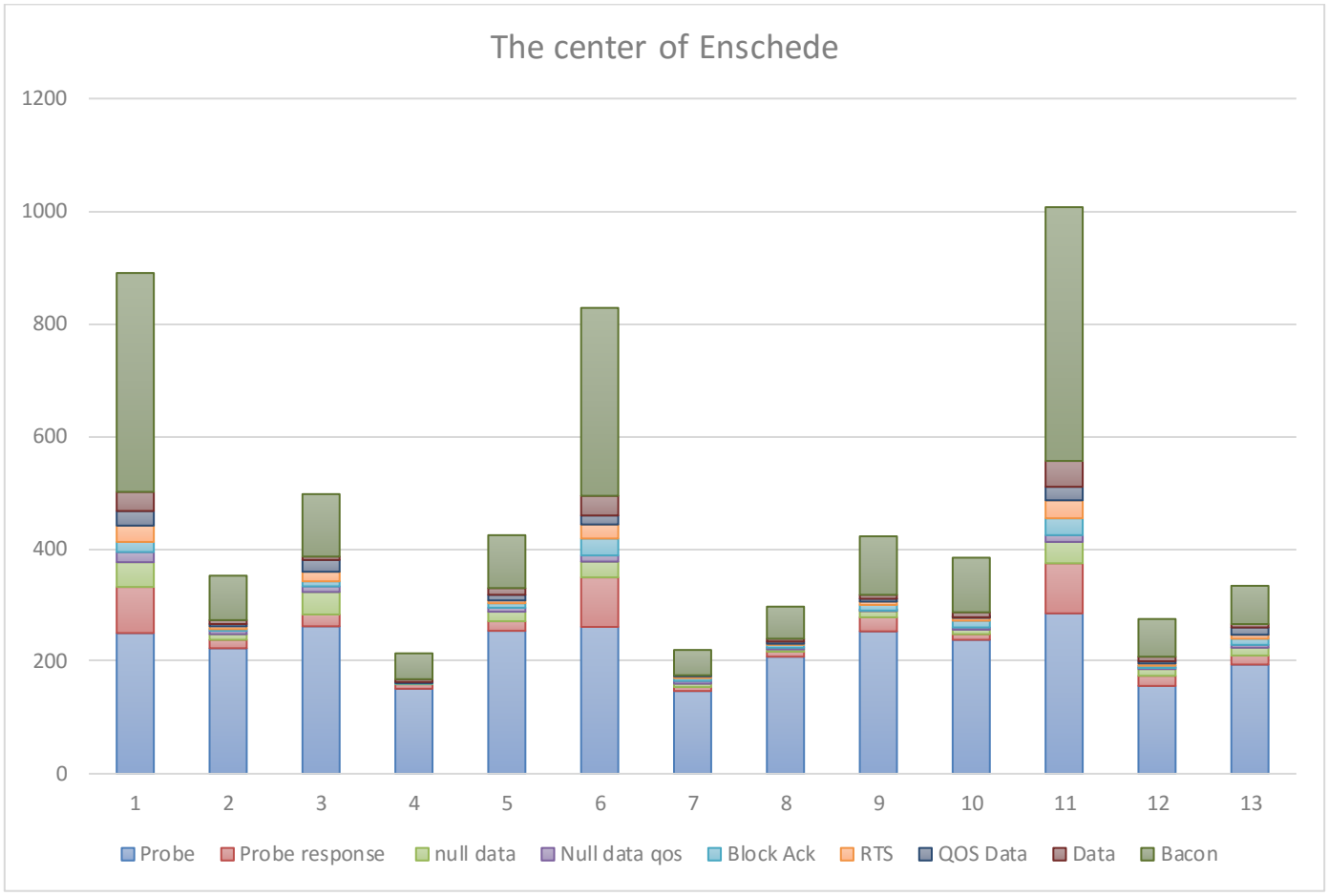

Figure 7: The center of Enschede