Wireless IoT and LAN: Wireshark Report

Xiaoyao Luo (5054702, xiaoyaoluo) Yifan Li (5145147, yli32)

March 10, 2020

Report contains 3 of maximum 4 pages.

1 Introduction

The main purpose of this project is that by using wireshark "sniffing" to gather WLAN information about the vendors of access point and station in the network. By extracting the data related to vendors from the data packet, the experiment finally summarized the proportion of vendors in different regions in Delft and analyzed it.

2 Method

In the project, data were captured around the dormitories and campus. The MAC address prefixes was extracted by python program and by comparing the information with Wireshark manufacturer database, corresponding vendor type was obtained and summarized into a histogram. By collating vendor company information, the project was able to determine which country's routers and mobile devices were more popular in the Netherlands.

2.1 Hypothesis

By analyzing the data collected in different regions, the project can obtain the types of vendors both the access point and station in the three regions and the number of users using such vendors in the region. For dormitory No.1 where the residents are mostly the same age as graduate students, the project initially assumed that Apple and Google would account for a high proportion. For dormitory No.2 where the residents are mostly middle aged and elderly people, since the project participants are not local people, it is speculated that there may be local brands or those with high popularity like Google or Cisco. For the campus, the preliminary hypothesis is similar the result of dormitory No.1.

3 Test setup

The project sniffs out all 802.11 frames by setting the built-in network card directly to Monitor mode. Here we use the python3.8 to analyze the collected data. And the Wireshark is running on Linux system (Ubuntu18.04), the python scripts is running on Windows system.

Considering that we need to collect the vendor information of the access points and stations, first of all, we choose to extract source addresses from beacon frames and request frames. Then we noticed that amount of probe request frame is too much less than that of beacon frame, which means there are only little stations. So we try to extract the destination addresses from the probe responses, which also carry the information about vendor types, the result shows we sniff more stations. Then here comes a question, based on the theory of connection process, the two methods we aforementioned should lead to the same result of stations, but actually, it shows great difference. To figure out this question, we try to track one specific mobile station, then it shows that after the station and access point finish the authentication and association process, the station does not send probe request any more, while the access point still sends the beacon frame. But it only explain why probe requests are much less than beacon frame, the question proposed before is still not clear.

In order to avoid the error caused by aforementioned question, we finally choose extract vendor type information of the station from both probe request frame and probe response frame, which means we choose the display filter "wlan.fc.type_subtype eq 4" and "wlan.fc.type_subtype eq 5". As for the information of access points ,we just choose to use "wlan.fc.type_subtype eq 8" as our filter to get the beacon frames then get the information of the vendors.

The project uses Wireshark to capture packets of WLAN data and use python program to extract the information about vendors in the packet and summarize it into bar charts. Through the investigation of different vendors' company information, the project also use excel to draw a pie chart of the information about the vendor company's nationality.

In the project, members captured three set of data around two dormitories and the campus teaching building which were analyzed respectively. All the "sniffing" data were obtained by walking in the area and shown in Table 1.

Region	Time(Minute)	Total data(Frame)
Dormitory No.1	88	120794
Dormitory No.2	70	146211
Campus	31	128977

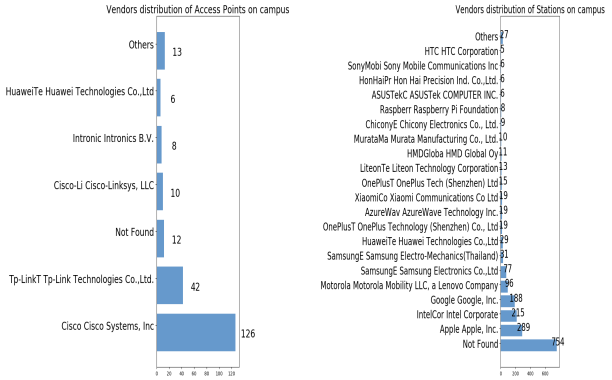
Table 1: Data information

4 Results and evaluation

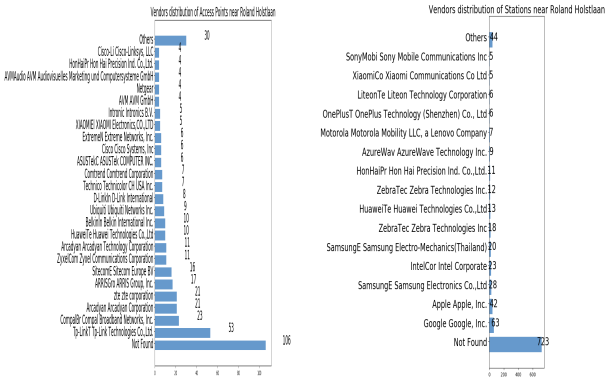
By extracting the vendors information of both access point and station in all three regions, Figure 1 shows the histogram of numbers of devices using corresponding vendors in three regions. Because a large number of vendors while sniffing only have one or two devices, if all displayed in chart the chart will be long. Thus in the histogram as shown in figure 1, all of this kind of vendors are classified into "others" vendor type but they are still taken into account when the nationality of the vendors is counted later.

Figures (a),(c),(e) from figure 1 show three different distributions of the Access Points' vendor types. On campus, Cisco's amount accounts for the vast majority, more than the other operators combined. That's easy to explain because TU Delft are all covered by Access Points provided by Cisco. And in the other two areas, the vendor types that could not be found in the Wireshark manufacturer database are much more than others. Besides the "not found" part, TP-Link, Compal, Arcadyan, ARRIS and zte are also the people's preferable choices.

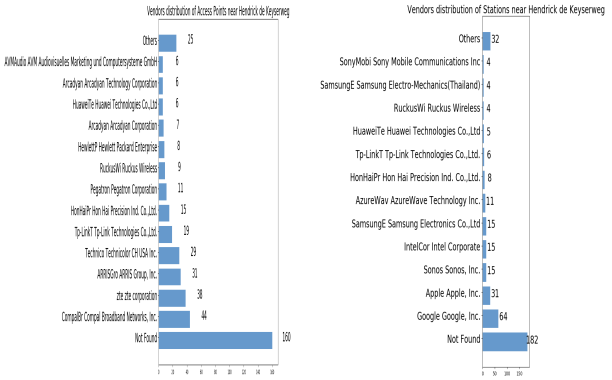
As for the distribution of stations in these three areas, according to online data from statcounter global stats which is shown in figure 2, Apple ranks first in the Netherlands, followed by Huawei and Xiaomi. Compared with figures (b),(d),(f), the experimental data included additional group of devices using vendors of Google, Inc. which accounted for a large proportion in all three regions. Apart from the unknown vendors, the arrangement of other vendors is basically similar the the data on the website. It is also clear from the figure that Apple, Google and Intel all have a large proportion in all three regions which is similar to the situation of people using devices in daily life. The difference is that the ratio of Apples vendor is higher in places like campus where there are more young people, but not in places like Hendrick where there are more middle-aged or even older people.



(a) Access points on campus (b) Stations on campus



(c) Access points near Roland Holstlaan (d) Stations near Roland Holstlaan



(e) Access points near Hendrick de Keyserweg (f) Stations near Hendrick de Keyserweg

Figure 1: Vendors distribution of Access points(left) and stations(right)

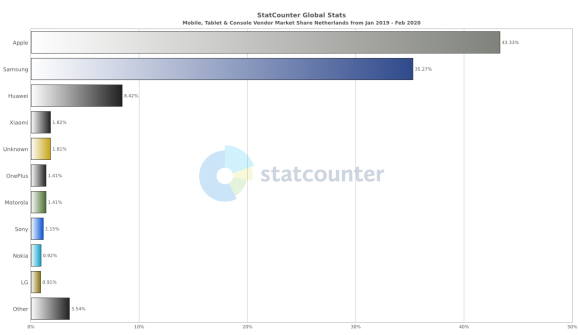
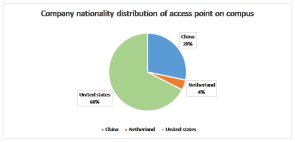
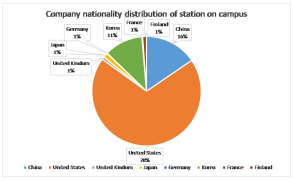


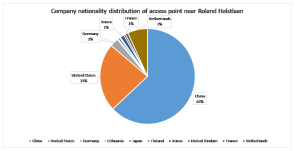
Figure 2: Vendors distribution of Netherlands from Jan 2019 to Feb 2020



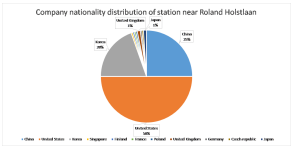
(a) Access points on campus



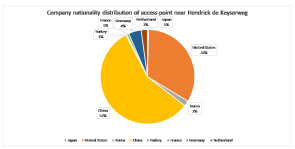
(b) Stations on campus



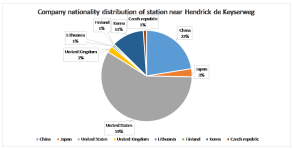
(c) Access points near Roland Holstlaan



(d) Stations near Roland Holstlaan



(e) Access points near Hendrick de Keyserweg



(f) Stations near Hendrick de Keyserweg

Figure 3: Vendors nationality distribution of Access Points(left) and Stations(right)

Figure 3 shows the nationality information of vendors both in access point and station, from the pie chart, American and Chinese vendors account for a significant proportion for both access points and stations with others such as France, Germany, Turkey or the republic of Czech accounting for less than 10 percentages. For access points, Dutch vendors have a percentage in each of the three regions while vendors of other countries only have one or two percent. For the station, the Korean vendors have exhibited a more obvious ratio and even in the Roland dormitory area South Korea's ratio and China's ratio are all about 20 percent. This means South Korea still leads the market in the production of mobile devices.

5 Conclusion

Through the analysis of vendors information in the project, the most striking result is that when analyzing the data, for both access points and stations, even if different databases are called, there still exist many MAC addresses that are not recognized by the database. This may require a database that are more optimized or updated for the growing number of MAC addresses typed. Based on the analysis of data, project also obtain the proportion of vendors for access points and stations in different regions. Combining with the analysis of nationality, for delft, American vendors account for a large proportion followed by China. For the local vendors in the Netherlands, they may only have one share of access points.