Daily Walks In Paris: A Practical Analysis of Wi-Fi Access Points

Guillaume Valadon, Florian Le Goff, Christophe Berger
Université Pierre et Marie Curie–Paris6
Paris, France
{*Guillaume.Valadon, Florian.Le-Goff, Christophe.Berger*}*@lip6.fr*

1. PRELIMINARY DISCUSSION

Over the past few years, it became much more easy and convenient to associate geographical coordinates to Wi-Fi Access Points (AP). Back in 2002, this activity known as *wardriving* involved to drive around with a laptop, a GPS receiver, and a PCMCIA wireless card. Nowadays, it may be directly performed on phones as they support Wi-Fi, using external GPS receivers.

This paper describes a *wardriving* campaign conducted using such devices. Our main motivation is to characterize the density of AP as well as their security modes. We chose to discover AP while walking in the streets, as would a regular user. This approach does not find all AP located in the district, but it precisely reflects the wireless environment. Therefore, the analysis of data provides realistic estimates of Wi-Fi parameters such as AP security modes or density. The latter could for example be used to find out if Wi-Fi based geolocation is doable in the districts.

Similar characterization work [1] exists but none of them analyze data gathered in Europe or France. Results presented here show that the Paris 802.11b/g landscape is driven by the French residential Internet access business due to following reasons: (1) most DSL subscriptions come with a dedicated modem/router that include a Wi-Fi AP; (2) some ISP deploy their own Wi-Fi AP from their customers routers.

2. DATA SET

The data was gathered during a rigorous wardriving campaign conducted in Paris 13th district from August to September 2007. The district was divided into areas in which the authors scanned streets by foot. In order not to alter measures, we tried to avoid going to the same streets more than once. We used Nokia N95 phones with external GPS receivers, and a dedicated wardriving software developed in Python[1]. For each AP, we collected the following information: geographic coordinates, reception level, security and connection modes, SSID[2], and BSSID[3]. Paris 13th district is approximately 7 km^2, but only 4 km^2 were scanned as we could not go to some areas such as hospital or private properties. During this campaign, 18313 AP were discovered. The data set is not publicly released, but Wi-Fi and GPS modules developed for Nokia phones are available at `http://www-rp.lip6.fr/~berger/pys60.html`.

3. CONNECTION MODE

As expected, AP are mainly configured in Infrastructure mode as it is the typical deployment of Wi-Fi networks. There is as few as 0.6%, exactly 115, of the total number of AP configured in Ad-Hoc mode. Among them, 24 are identified as *hpsetup*: the factory SSID of HP printers and laptops. Remaining ones belong to an ongoing OLSR[4] experiment in the district, and to personal wireless music centers from Philips. All other SSID are unique and cannot be classified.

4. AP DENSITY

In January 2006, there were around 1900 AP/km^2 in Manhattan [1]. Earlier this year (2007), there were close to 3000 AP/km^2 in Tokyo urban areas[5]. In the Paris 13th district, there are between 2612 and 4700 AP/km^2. In the first result, the total number of observed AP was divided by the size of the district. In the second one, it was divided by the size of the scanned zone. As described earlier, some ISP use their customers AP to broadcast their own SSID (*freephonie*, and *Neuf WiFi*). This causes some AP to be counted

*CoNEXT'*07, December 10-13, 2007, New York, NY, U.S.A.

[1]Python for S60 devices; `http://pys60.sf.net`
[2]Service Set IDentifier; the network name.
[3]Basic Service Set IDentifier; unique ID of the AP.
[4]a protocol for mesh networks; see RFC 3626.
[5]private conversation with a PlaceEngine [2] Team member.

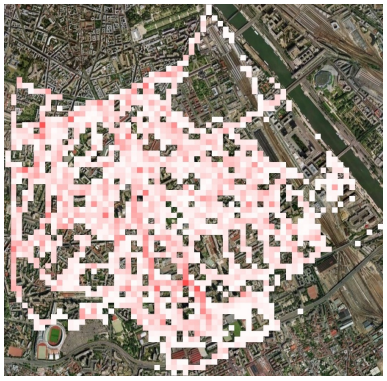

Figure 1: Density in Paris 13th

Mode	%	Mode	%
Open	9.9	WPA	18.1
WEP	41	WPA-PSK	31
Open; No ISP	5.5	WPA; No ISP	0.2

Table 1: Security modes in Paris 13th

twice. After the removal of these SSID, densities are 2049 and 3586 AP/km^2.

In our data set, we observed no clear correlation between AP and population density. However, as shown in Figure 1, we observe that the $50m * 50m$ squares with the highest density (in red) are located around tall buildings or avenues where there is a higher concentration of apartments.

5. SECURITY MODE

Five years ago, a wardriving survey conducted by one of the authors in five Paris districts revealed that most AP were open (encryption-free). Today, only 9.9% are, see Table 1. However, corresponding SSID reveal that 10 ISP use open AP as part of their business, and force their users to authenticate on a captive portal. If these ISP are removed, there is only 5.5% of open AP. We estimate that almost all of them are still using their default factory setup. Even though WEP has proved to be unsafe about five years ago, it is still used by 41% of AP. This shows that WEP is still hanging on whereas better modes exist. The percentage of AP using WPA-PSK is higher than expected. This is likely to be related to the fact that most French ISP are shipping AP configured by default with WPA-PSK. On the other hand, the WPA (also known as WPA-Enterprise) scheme represents 18.1% of AP. This is surprising as it is generally used to secure private company networks. In fact most associated SSID correspond to an ISP using customers' AP to extend their own Voice over Wi-Fi network. Once removed, WPA only accounts for 0.2% of AP.

6. MANUFACTURERS

The classification of AP by manufacturers shown in Table 2 was produced by comparing BSSID to the Organizational Unit Identifier (OUI) database [6]. As expected, well known network vendors are ranked after AP shipped with DSL subscriptions, such as Freebox SA and neuf cegetel. It is interesting to note that 42% of AP are labeled as *Unknown*; their corresponding BSSID are not in the OUI database. However, sorting out the AP by SSID, security modes, and consecutive BSSID shows that 5367 of these AP are associated with AP supplied by the third French ISP (Freebox SA). Consequently, the classification by manufacturers witnesses that 68% of AP where shipped by ISP.

%	Name	%	Name
42	Unknown	4	FreeBox SA
11.6	Hon Hai Prec.	3	Cisco-Linksys
8.5	USI	2.2	D-Link Corp.
7.8	TECOM Co.Ltd.	2.1	NETGEAR Inc
6.9	neuf cegetel	1.8	ASKEY COMP. Co.

Table 2: TOP 10 manufacturers in Paris 13th

7. SSID

In general, analysis of network names does not give much information by itself. However, they are fairly good indicators that AP use their default factory settings. In our data set, we identified that around 5% of AP are in this situation. Among the first SSID, three of them correspond to AP shipped by ISP: *freephonie*, *Neuf WiFi*, *N9UF_TEL9COM* and *THOMSON*. The remaining three SSID are the factory default of popular manufacturers: *NETGEAR*, *linksys*, and *dlink*.

8. FUTURE WORK

Following work will study the evolution of parameters described in this paper. Specifically, we want to study if the repartition of the security schemes is stable or not. Furthermore, we would like to check if some AP are disappearing or if we can only observe a constant expansion.

9. REFERENCES

[1] K. Jones and L. Liu, "What Where Wi: An Analysis of Millions of Wi-Fi Access Points," in *Proceedings of 2007 IEEE Portable: International Conference on Portable Information Devices*, May 2007.

[2] "PlaceEngine," http://www.placeengine.com.

[6] http://standards.ieee.org/regauth/oui/oui.txt