Differences in RSSI Readings Made by Different Wi-Fi Chipsets: A Limitation of WLAN Localization

Gough Lui
School of Photovoltaics and Renewable Engineering
Univeristy of New South Wales
Sydney, Australia
gough@student.unsw.edu.au

Thomas Gallagher, Binghao Li, Andrew G. Dempster, and Chris Rizos
School of Surveying and Spatial Information Systems
University of New South Wales
Sydney, Australia
t.gallagher@unsw.edu.au

Abstract—**Wi-Fi positioning has found favour in environments which are traditionally challenging for GPS. The currently used method of Wi-Fi fingerprinting assumes that the devices used for training and locating perform identically. We have undertaken an experiment to determine how different devices behave in an empirical controlled test to identify the challenges and limitations which Wi-Fi fingerprinting positioning systems will face when deployed across many devices. We found that they performed significantly differently in respect to the mean reported signal strength – even those which came from the same vendor. We also found that multiple samples of the same device do not perform identically. Furthermore, it was found that certain devices were entirely unsuitable for positioning as they reported signal strength values uncorrelated with distance from the transmitter. Some other devices behaved in a way that made them poor candidates for use in fingerprinting. Temporal patterns were found in some wireless cards which suggest that filtering should be used. The tests also found that the use of 5GHz band signals had the potential to improve the accuracy of Wi-Fi location due to its higher stability compared to 2.4GHz. Ultimately however, the accuracy of Wi-Fi fingerprinting is limited due to many factors in the hardware and software design of Wi-Fi devices which affect the reported signal strength.**

WLAN localization; fingerprinting; limitations; Wi-Fi chipsets; RSSI differences

I. Introduction

GPS is widely accepted as a ubiquitous positioning system as, in most conditions, it is accurate, reliable and available. It has supported the tremendous growth that has been seen in the Location Based Services (LBS) market in the past few years, being used in a wide variety of mass-market applications such as the well-known Google Maps [1], or Foursquare [2]. However, the use of LBS is still limited to outdoor environments, where GPS can provide a location with reasonable accuracy. In environments such as urban canyons or indoors, where consumers of LBS spend most of their time, no acceptable location can be provided.

Many technologies have been investigated to bridge the gap and bring positioning indoors, such as a combination of A-GPS, accelerometer and magnetometer [3], Bluetooth [4], Ultra-wideband [5], ZigBee [6], GSM [7], or even high-sensitivity GNSS [8]. Wi-Fi is another of them, and is considered as the most promising one as the infrastructure and user equipment is already widely available, and it is able to deliver accuracies in the range of a few meters. Wi-Fi fingerprinting was pioneered in [9], and has since attracted considerable interest, mainly focused on increasing the accuracy of the technique. Fingerprinting consists of two phases. The first consists of surveying the desired area of coverage to record Wi-Fi scan results at selected reference points, the scan results containing the MAC address of access points and their Received Signal Strength Indicator (RSSI). When the user requires his or her position, the device scans the Wi-Fi network and compares the result with all the scan results stored previously in the database. The closest match is then returned to the user.

Most of the Wi-Fi fingerprinting algorithms which match the users scan result to elements of the database have been developed on the assumption that the devices used for the training and positioning phase perform identically. That is a strong assumption given the extremely wide array of Wi-Fi chipsets on the market built in a variety of devices such as laptops, smartphones, USB-dongles, etc. A few papers have investigated this issue, such as [10] and [11]. Haeberlen et al. [10] tested three chipsets by various vendors and found out that they reported RSSI in different ways, but that a linear relationship appears to exist between the ways these chipsets reported these values. Tao et al. [11] observed that there is a linear relation between transmission power and the RSSI reported by 802.11 hardware.

In this paper, we have undertaken an experiment to determine how different devices behave in a practical, controlled test with distances from the Access Point (AP) ranging from 0.3m to 35m in indoor and outdoor environments to identify the challenges and limitations which Wi-Fi fingerprinting positioning systems will face when deployed across many devices. In that experiment, particular care was taken to try to minimize the impact of environmental and temporal variability on the results, focusing purely on how the hardware outputs the RSSI values. We found out that different Wi-Fi devices perform significantly differently, even those which have come from the same vendor. We also found that even two identical models of Wi-Fi chipsets do not perform identically. Our conclusion is that significant calibration is needed in order to maintain reasonable accuracy across several devices. Another conclusion is that some devices are entirely unsuitable for positioning purposes as they report bogus RSSI values. Some other devices behaved in a way that makes them poor candidates for a positioning system, such as RSSI "caching", small gradient or limited resolution in RSSI values. A few chipsets operating in the 5GHz band were also tested. It was observed that the use of the 5GHz has the potential to increase the accuracy of Wi-Fi positioning systems.

The remainder of this paper is organized as follows. In section 2, we present the testing methodology and devices used for the tests. In section 3, we present the results of these tests. Finally in section 4, a discussion of the reasons that the cards output RSSI differently is conducted.

II. Testing Methodology

A. *Devices used for testing*

A variety of Wi-Fi devices including USB dongles, laptops, mobile phones and Wi-Fi tags were tested. Table 1 presents the list of devices tested, and their chipsets when known. A Belkin Play Wireless Dual-Band Access Point was used. The USB wireless cards were tested using the latest available drivers from the vendors on a BenQ R55UV10 laptop, running Windows XP Service Pack 3. The signal strengths were logged using InSSIDer Version 1 [12], an open-source software developed by MetaGeek. The embedded cards were tested using the same software combination. Software was developed to test the Android phone, and the Roving Networks tag. The Nokia N95 was tested using PyNetMony [13].

B. *Testing methodology*

The AP was set up at a fixed location on top of a plastic bin and a set of boxes. The device under test was placed on top of an identical plastic bin on a movable trolley, such that the height of the base of the AP and device under testing was identical. The trolley was moved to one of 15 distances, namely 0.3m, 0.5m, 0.8m, 1m, 1.5m, 2m, 2.5m, 5m, 7.5m, 10m, 15m, 20m , 25m, 30m , and 35m. The RSSI from the Wi-Fi device was then recorded for 5 minutes before being moved to the next distance. Of these 5 minutes, only 4 minutes of data were used, as the cart was moved by the tester in the remaining minute.

This was repeated for all the devices and in two environments, indoors and outdoors. The indoor environment chosen was the fourth floor hallway of the Electrical Engineering building at the University of New South Wales. The outdoor environment chosen was one of the pathways in the Quadrangle, also at the University of New South Wales. It is important to note that the tests took place over the summer session, when pedestrian traffic was much reduced compared to normal, hence reducing the effect of human bodies on the measurements.

Finally, the orientation of the devices under test was fixed in order to minimize the influence of orientation. USB dongle format devices were inserted in a D-Link USB extension cable which kept the dongle vertical. Other devices, such as phones and larger format wireless adapters were laid down flat.

TABLE I. List of Devices Tested

Id	Manufacturer and Model	Chipset
1	Diamond Digital A101	Envara WiND502
2	Netgear WG111v2	Realtek (RTL8187L)
3	Netgear WPN111	Atheros (AR5523A/AR2112A)
4	Netgear WG111U	Atheros (AR5523A/AR5112A)
5	D-Link DWA-140	Ralink RT2870
6	D-Link DWL-122G	Ralink RT2570
7	Netgear MA101	Atmel AT7650x
8	Billion BiPAC3011G	Zydas (ZD1211)
9	Belkin Play USB	Broadcom (BCM4323)
10	HP2133 Mini Notebook	Broadcom (BCM4312)
11	BenQ Joybook R55UV10 laptop	Intel Centrino 3945ABG
12	HP Pavilion dv4000 laptop	Intel Centrino 2200BG
13	HP Elitebook	Intel Wi-Fi Link 5300N
14	Asus EEEPC 701	Atheros (AR5006UG)
15	Nokia N95	Unknown
16	HTC Dream	Texas Instruments WL1251B
17	Roving Networks Wi-Fi Tag	Unknown

At the least 100 raw RSSI readings were obtained per position, except for the Nokia N95 phone and the Roving Networks tag, which didn't allow a refresh rate high enough to achieve this.

III. Results

A. *Differences in RSSI readings*

Fig. 1 and 2 present the average of all RSSI readings at each of the test points for all devices. Fig. 3 provides the legend for both fig. 1 and 2. From a quick observation of these figures, it can clearly be seen that there are big differences between the values reported by the individual cards at the same points. In the indoor test, differences of as much as 30dBm can be observed in averaged RSSI at the same point. As the time of the test was different for each device, there is of course an impact of temporal variations on the results, such as people walking in the test zone, opening and closing of doors, etc. However, they only cannot explain such big differences in the readings. Indeed, in the outdoor test where temporal variability of the environment was greatly reduced compared to the indoor test, the same order of differences was observed.

It could be hypothesized that cards with chipsets from the same vendor will perform similarly. If this were the case, it could make the calibration effort much easier. However, a close look at fig. 1 and 2 show that this is not the case. In the outdoor test, a difference of 20dBm at 2.5m was observed for the Intel series of Wi-Fi cards, commonly found in laptops; a

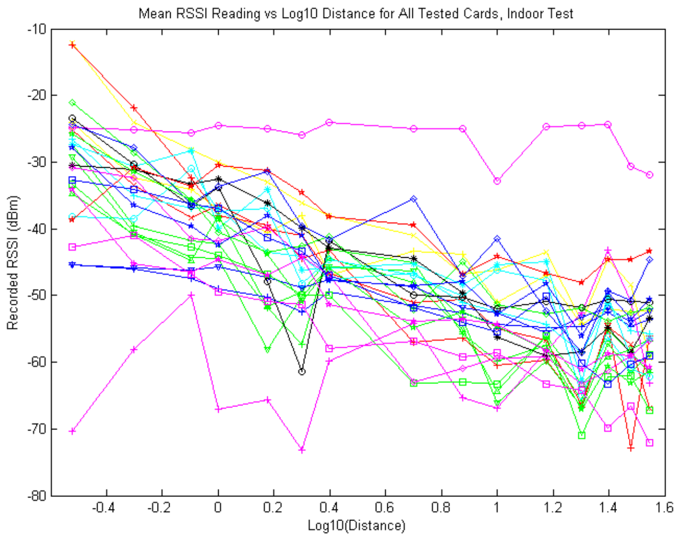

Figure 1. Recorded RSSI vs. Log10(distance) for all devices – indoor test

difference of 16dBm at 7.5m was observed for the Broadcom devices (Broadcom and Belkin branded); and a difference of 15dBm was observed at 1m for the Atheros devices (Atheros and Netgear branded). There is no clear evidence to suggest that different generations of devices from the same chipset vendor will perform similarly and thus each unique chipset generation will have to be catered for.

Even more interesting is when observing identical models of the Wi-Fi cards. Fig. 4 plots the averaged RSSI at each test point for the 3 Billion branded identical cards. As can be seen, the cards behave as expected at some points with a very similar averaged RSSI, but differ significantly at other points (14dBm at 0.5m for instance). This is despite careful testing setup ensuring the distances and orientation remained as similar as possible. It suggests that there may be some variances between samples of the same wireless device, and also that calibration cannot be accurately done without specialized test equipment due to variances which may exist in the testing environment.

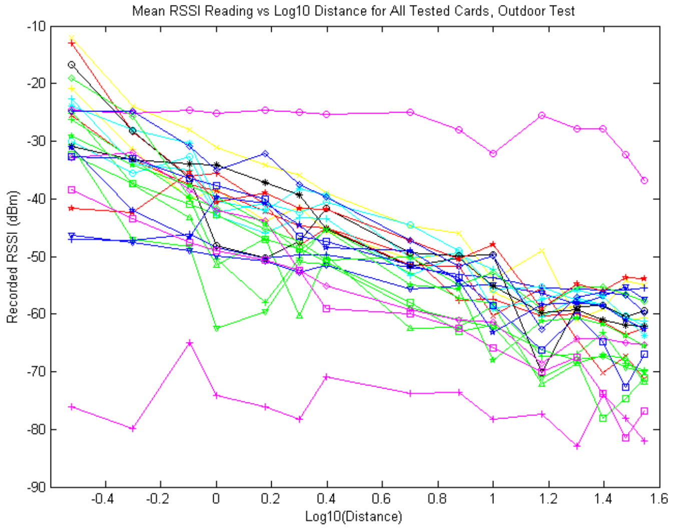

Figure 2. Recorded RSSI vs. Log10(distance) for all devices – outdoor test

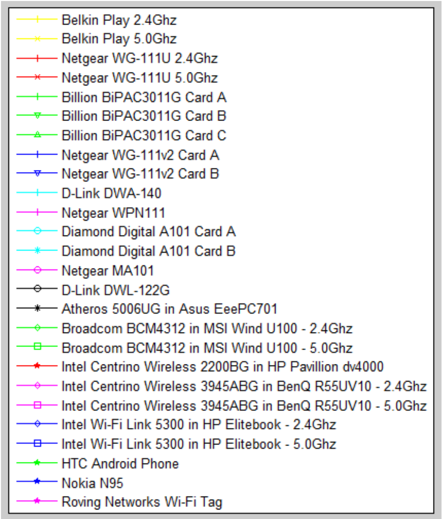

Figure 3. Legend for fig. 1 and 2

B. *Features of interest for RSSI fingerprinting*

1) *Peculiar behavior of some devices*

Fig. 5 shows the temporal RSSI trends for selected devices with peculiar behaviour which will impact on the accuracy of Wi-Fi positioning systems. Of note is that there is behaviour that suggests a “dropout” of data – where the RSSI suddenly falls and recovers, most commonly occurring in 2.4GHz, there are oscillations in the signal strength values, most obvious in the Intel series of cards. There is also evidence of “signal strength caching” on the Netgear WG111U where signals seem to be stable for a large period of time before changing, and finally differences in reported RSSI increments with the D-Link DWA-140 where the RSSI changes in increments of 2dB. Some other cards show a combination of all these. In all cases, the use of filtering algorithm which cut out spurious data can be seen to be highly recommended in light of this behaviour.

Some cards also appear to be completely unadapted to Wi-Fi positioning, as can be seen on fig. 1 and 2. In particular, the

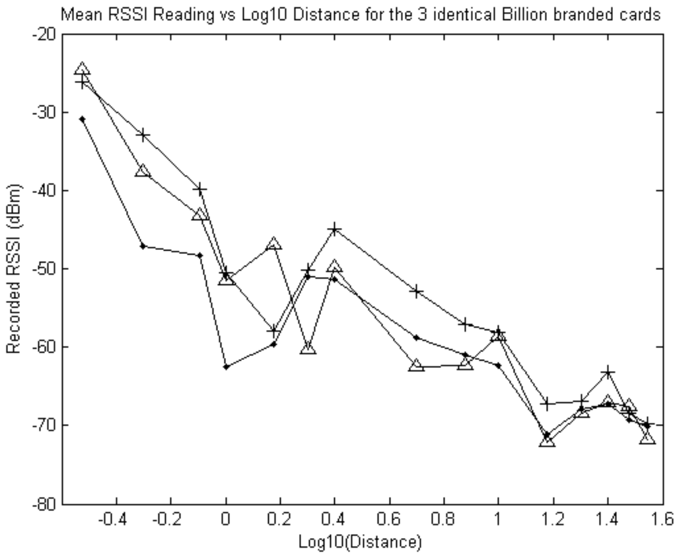

Figure 4. Three identical devices – outdoor test

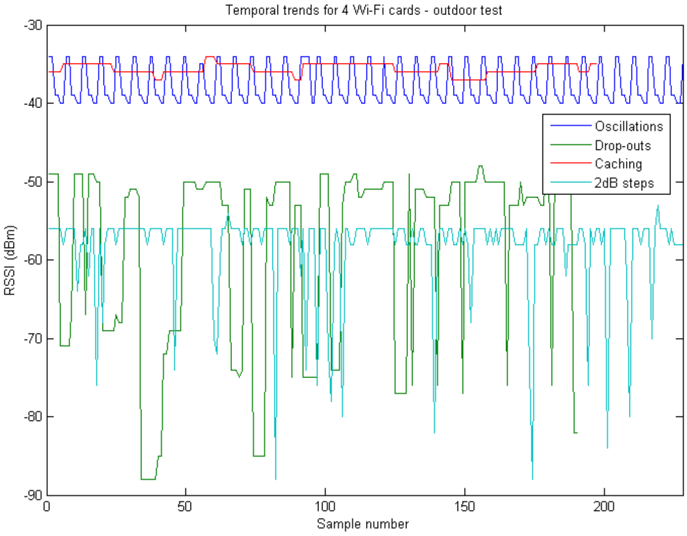

Figure 5. Illustration of peculiar behavior observed in some devices

Netgear MA101 and Netgear WPN111 do not report sensible RSSI values. The trend is present in both indoor and outdoor testing and is hence shown to be a software or hardware issue. It is of interest to note that the WPN111 and the WG111U both use a similar design with the same baseband processor but a different RF chip and different drivers, yet one of them is able to report signal strengths correctly.

2) Gradient of RSSI variations

From the outdoor testing data, a linear fit between RSSI and the logarithm of distance was made using polyfit in Matlab as the data is expected to have a linear correlation. The gradient for all devices is summarized in Table 2. The lines of the table with several sub-lines indicate that there were several identical devices of that type.

As can be seen, most of the cards behave similarly with a gradient between -15 and -20 dBm/log10(m). Some devices however, have a much lower gradient such as the Intel Centrino 2200BG or the Netgear WPN111. These cards are obviously not suited for Wi-Fi fingerprinting, as this technique takes advantage of big variations of signal strength within a small distance range. Fig. 2 shows many deviations from the expected linear relationship between RSSI and the logarithm of distance, which are can be due to changes in the environment between tests and eventual non-linearities in the devices themselves. Despite all care ensuring the test setup was identical for every run, the deviations suggest that calibration techniques in an open environment will still be subject to variations and limitations in accuracy.

3) Standard deviations of RSSI

Table 2 also shows the mean of the standard deviations recorded by each card over all distances for indoor and outdoor testing. For Wi-Fi positioning applications, the lower the standard deviation, i.e. the more stable the readings are, the better it is, as there will be a higher probability that when the user requests his position, his scan results will be similar to the ones stored in the database.

TABLE II. GRADIENTS AND STANDARD DEVIATIONS

Id	Gradients outdoor	Average STD indoor (dBm)	Average STD outdoor (dBm)
1	-14.964 -18.066	5.239 3.905	5.650 4.578
2	-5.087 -5.283	1.175 1.019	1.751 1.651
3	-2.594	12.339	13.460
4	-20.741 (2.4GHz) -20.203 (5GHz)	3.067 (2.4GHz) 0.861 (5GHz)	3.480 (2.4GHz) 0.655 (5GHz)
5	-15.930	7.124	8.224
6	-17.143	1.621	1.321
7	-3.815	5.660	6.285
8	-17.878 -14.067 -18.612	9.089 7.770 9.343	5.501 9.658 10.013
9	-16.638 (2.4GHz) -20.647 (5GHz)	5.438 (2.4GHz) 0.531 (5GHz)	8.706 (2.4GHz) 0.143 (5GHz)
10	-15.414 (2.4GHz) -20.647 (5GHz)	3.271 (2.4GHz) 0.533 (5GHz)	2.231 (2.4GHz) 0.605 (5GHz)
11	-17.600 (2.4GHz) -18.319 (5GHz)	8.256 (2.4GHz) 2.570 (5GHz)	8.091 (2.4GHz) 1.892 (5GHz)
12	-9.340	6.238	8.105
13	-18.462 (2.4GHz) -19.089 (5GHz)	12.978 (2.4GHz) 2.593 (5GHz)	12.961 (2.4GHz) 2.417 (5GHz)
14	-17.209	4.586	3.500
15	-13.338	5.867	3.553
16	-17.461	1.858	1.261

In this aspect, the cards diverge greatly. In the 2.4GHz band, some devices have very low standard deviations, such as the HTC Dream, or the Netgear WG-111v2 cards. Others output very unstable values, such as the Intel Wi-Fi Link 5300N or the Netgear WPN111.

It can also be seen that the variances of the 5GHz signals were consistently lower than the 2.4GHz signals. This could possibly be attributed to less interference in the 5GHz band from other devices and no co-channel users compared to 2.4GHz. It could also possibly be attributed to propagation effects. This result suggests that the use of the 5GHz band for Wi-Fi positioning has the potential to improve the accuracy of fingerprinting.

IV. DISCUSSION

Antenna design has the potential to affect the RSSI received due to several factors. Firstly, practical antennas are not isotropic, and certain antennas with high gain may not even be omnidirectional. This leads to a difference in signal strength with respect to the device's orientation to the access point. Differences in antenna polarization due to the orientation also have the potential to reduce the signal strength due to polarization mismatch. High gain antennas also will increase the received signal levels of some nearby access points, while possibly reducing the signal strength of others due to the reduced beamwidth angles. This testing, therefore, is testing the complete implementation of the device, rather than solely the chipset, and simple calibration by compensating for a device's offset and gain may not fully compensate for differences in the antenna's radiation pattern.

Furthermore, more advanced chipsets feature the use of multiple antennas – especially in the use of multiple-in multiple-out (MIMO) based Wireless N cards which commonly feature two or more antennas; however, this issue affects even older wireless G cards with diversity reception. The reason for this is that the way the card reports the signal may be related to both antennas – when compared with a device with only a single antenna or a different antenna design, it can be expected that there are differences between the signal strengths as there are essentially two or more receivers at slightly different locations within the same device. Information was sought from manufacturers about how the signal strength is calculated from the received signals at multiple antennas, however, all manufacturers consulted have not replied. It could reasonably be expected that there is some variation between different manufacturers and the way they process the signals.

Different chipsets may be built with different RF front-end designs. There are Wi-Fi chipset designs which involve an Intermediate Frequency step, while some tout a "zero-IF" solution and the way they extract RSSI is somewhat different. Therefore the RSSI reported is dependent on design choices made by the manufacturer.

As there is no fixed standard which manufacturers are required to follow, signal strength indications are to be used for indication only and do not indicate the true absolute signal strength received. These values are reported by a piece of software which allows the operating system to use the wireless card – i.e. the drivers. These drivers feature the role of controlling and reporting the status of the card, and therefore the strengths reported by the card are highly dependent on the mapping which is established between hardware AGC values and RSSI values reported by the driver.

Different device design and usage by end users could also lead to different signal levels due to human influences. Furthermore, differences in the environment from interfering access points and devices, as well as human traffic and changes in furniture layout will cause different RSSIs to be received in the same location.

V. Conclusion

From the testing, we can conclude that there are significant differences between Wi-Fi devices. Devices from the same vendor were not found to perform similarly, and devices of the same model could not be proven to perform identically. Furthermore, it was found that some devices were not able to report valid or useful RSSIs which makes them incompatible with Wi-Fi Fingerprinting, while other devices have unusual temporal patterns which makes them undesirable for this application. From this, we can conclude that calibration is necessary if a variety of different Wi-Fi devices are used; however, there are difficulties in producing an accurate calibration given the variance observed in the same model of device. Also, it is necessary to employ filtering techniques in order to improve the accuracy in the presence of "RSSI dropouts".

We have also found that 5Ghz band signals seem to be much more adapted to this application than 2.4Ghz signals, and could improve the overall accuracy of the system. This is possibly due to a lack of co-channel interference and different propagation modes.

It was also argued that there are many factors which can affect the RSSI returned by a Wi-Fi device, including the antenna design, hardware design, drivers and the environment. Given the large number of factors governing the received RSSI, calibration is unlikely to be able to compensate for all of them, leading us to conclude that there is an inherent limit to the accuracy of a Wi-Fi positioning system especially when multiple devices are used.

References

[1] Google Maps, http://maps.google.com

[2] Foursquare, http://www.foursquare.com

[3] D. Gusenbauer, C. Isert, and J. Krosche, "Self-contained indoor positioning on off-the-shelf mobile devices", *Indoor Positioning and Indoor Navigation 2010*, pp. 1-9.

[4] S. Feldmann, K. Kyamakya, A. Zapater, and Z. Lue, "An indoor Bluetooth-based positioning system: concept, implementation and experimental evaluation", *International Conference on Wireless Networks,* 2003.

[5] C. Zhang, M. Kuhn, B. Merkl, A.E. Fathy, and M. Mahfouz, "Accurate UWB indoor localization system utilizing time difference of arrival approach", *IEEE Radio and Wireless Symposium,* pp. 515-518, 17-19th Oct. 2006.

[6] M. Sugano, "Indoor localization system using rssi measurement of wireless sensor network on zigbee standard", *Wireless and Optical Communications,* pp. 1-6, 2006.

[7] V. Otsason, A. Varshavsky, A. LaMarca, and E. de Lara, "Accurate GSM indoor localization", *Proceedings of Ubicomp 2005,* pp. 141-158, 2005.

[8] J. Zhang, B. Li, and C. Rizos, "Evaluation of high sensitivity GPS receivers", *2010 Int. Symp. On GPS/GNSS,* pp. 410-415, Taipei, Taiwan, 26-28th October 2010.

[9] P. Bahl, V.N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system", *Proceedings of Infocom*, pp. 775-784, 2000.

[10] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki, "Practical robust localization over large-scale 802.11 wireless networks", *Proceedings of the 10th annual international conference on mobile computing and networking MobiCom'04*, September 26 – October 01, 2004, Philadelphia, PA, USA.

[11] P. Tao, A. Rudys, A.M. Ladd, and D. S. Wallach, "Wireless LAN location-sensing for security applications", *Proceedings of the second ACM workshop on wireless security (WiSe)*, September 2003, San Diego , CA, USA.

[12] inSSIDer, http://www.metageek.net/products/inssider/

[13] PyNetMony, http://sites.google.com/site/pynetmony/home/