

## TO LOCALISE OR TO BE LOCALISED WITH WIFI IN THE HUBEI MUSEUM?

Edward Verbree<sup>a</sup>, Sisi Zlatanova<sup>a</sup>, Karl van Winden<sup>b</sup>, Eva van der Laan<sup>b</sup>, Antigoni Makri<sup>b</sup>,  
Li Taizhou<sup>c</sup>, Ai Haojun<sup>c</sup>

<sup>a</sup> Delft University of Technology, Faculty of Architecture and the Built Environment  
e.verbree@tudelft.nl; s.zlatanova@tudelft.nl

<sup>b</sup> Delft University of Technology, MSc Geomatics

<sup>c</sup> School of Computing, Wuhan University

ISPRS Working group IV/7

**KEY WORDS: WiFi Fingerprinting, WiFi Monitoring, Indoor Localisation**

### ABSTRACT:

Indoor localisation is in demand for a variety of applications within the built environment. An overall solution based on a single technology has not yet been determined. The aim of this paper is to gain insight on Signal Strength monitoring by a special kind of WiFi Monitors in comparison to the commonly known fingerprinting method for the purpose of a 3D indoor navigation system. Two different WiFi based localisation techniques are tested during the MSc Geomatics DaRen Syntheses Project in the Hubei Provincial Museum, China.

The first method detects the beacon frames sent by smartphones, laptops and other WiFi enabled devices in range using Libelium Meshlium Xtreme monitors. Their MAC addresses and the signal strength is measured by the Meshlium Xtreme and stored on an external database. We call this method WiFi monitoring. The second method a WiFi enabled device, like a smartphone, measures the signal strength of multiple WiFi Access Points in range to localise itself based on a previously created radio map. This method is known as WiFi fingerprinting.

Both methods have some advantages and disadvantages. Advantages of the common way of WiFi fingerprinting are that the implementation costs are relatively low, because it is usually possible to use (a part of) the existing WiFi AP infrastructure. WiFi fingerprinting can reach a relatively high accuracy in the order of magnitude of meters. Finally, the location granularity can be adjusted to what is necessary for the purpose of the indoor localisation. This makes it employable for a wide range of purposes.

The question remains how suitable these methods are for a 3D indoor navigation system for the Hubei provincial museum. One important aspect is the localisation-granularity necessary for the application. In a museum it is not necessary to know the exact X,Y position of a user (such high accuracy is unnecessary), more important is to know in which room the user is located so the information on exhibitions can be presented and the starting point of the navigation can be determined.

Both methods can track the user and tell the room he or she is located at. Although WiFi smartphone monitoring may have a low update frequency it is still suitable for a navigation system for a museum since visitors usually spend more than a couple of minutes within a room.

### 1. INTRODUCTION

The research was focused on two Wi-Fi based localization methods, Wi-Fi monitoring and Wi-Fi fingerprinting using the existing WLAN infrastructure. The first method detects the beacon frames sent out by mobile devices, laptops and other Wi-Fi enabled devices in range using Libelium Meshlium Xtreme monitors - Wi-Fi monitors (Libelium, 2013) while in the second one a mobile application receives signal strength measurements from multiple access points and compares them with the values obtained in a previous (training) phase. The main question that needs to be investigated is how suitable these methods are for a context aware 3D indoor navigation system for the Hubei Provincial museum. The system demands a few requirements of the localisation part. The most important requirement is to provide the location of the user to the application so that the right starting point in the navigation network to be assigned. A second requirement is to provide the room in which the user is located to be able to inform the user on the exhibits in that room. Moreover, the system has to be able to provide the real time location of the user. Besides these user- and application- requirements, there is also a requirement

from the museum point-of-view. The museum should be given insight on the behaviour of people and the amount of people present in the museum.

### 2. WIFI MONITORING

The Meshlium Xtreme router launched by Libelium company is the Wi-Fi monitor that is used in the current project. Meshlium Xtreme is a multiprotocol router for wireless sensor networks designed to connect ZigBee, Wi-Fi and Bluetooth sensors to the Internet through 3G connectivity. It allows the detection of any device working with Wi-Fi or Bluetooth interfaces, such as iPhone and Android devices. In this research the device is going to be used to detect mobile devices through their Wi-Fi connection. The information read from each user by the Wi-Fi monitor contains:

- The MAC address of the wireless interface, which allows identifying it uniquely.
- The strength of the signal (in RSSI quality (0-100%) from signal strength -90 dBm and -40 dBm)
- The vendor of the Mobile device (Apple, Nokia, etc)

- The Wi-Fi Access Point where the user is connected (if any). Users not connected to an AP will be showed as "free users". The recorded data can be stored in a local or an external database. The Wi-Fi monitor is plugged into the power, which allows the administrator to read the data when connected to the device. However, if the Wi-Fi monitor is connected to the internet, the records can be sent to an external database. This makes it possible for the administrator to access the data from any place when provided with Internet connection (Libelium, 2013).

During the testing phase the benefits and drawbacks of the Wi-Fi monitors were revealed. The major issue with the Wi-Fi monitors is that the interval between two successful scans of the same mobile device is large (a couple of minutes). The scanning cycle of the Wi-Fi monitors is set at 5 seconds in most cases and even 2 seconds at times, but still the interval between two scans is between a minute and a couple of minutes. This is most likely due to the active scanning of the mobile devices and the interval between probe requests. Probe requests are the active scans by the mobile device. "During active scan, the client tunes its IEEE 802.11 radio to the channel being scanned and broadcasts a probe request in order to listen to any available probe responses from APs on the specific channel with the matching SSID" (Sidiropoulos et al., 2012). A directed probe requests let the client send a name-specific SSID request on which the specific SSID will response. A broadcast probe with a null SSID will cause all the APs to respond and these requests can be picked up by the Wi-Fi monitor. For a mobile device that is asleep, it sends out a probe request every minute. When the mobile device is in stand-by it sends out a request every 4-6 seconds. Only manual scanning for networks by the user can increase the interval (Cisco, 2013). The interval between the probe requests and the scanning cycle of the Wi-Fi monitors causes the Wi-Fi monitors to miss some requests, which leads to larger intervals than necessary. For localization purposes the current interval between two scans is too big, because within a minute a user can already be moved from one room to the other. Also it is desirable for a localization system that all Wi-Fi monitors, in our case two, to scan the user at the same time. This cannot be guaranteed with our Wi-Fi monitors. A smaller interval between consecutive probe requests would be a solution to scan the mobile devices more often. According to Musa and Eriksson (2012) a smaller interval can be achieved by "opportunistic AP emulation". Besides the broadcast probes a mobile device sends out frequently, it also frequently sends out directed probe requests for a specific SSID that it has been associated to in the past. The idea is to change the SSID of the Wi-Fi monitor in a SSID that the user has used in the past. In general this SSID can be well known providers that are in the memory of many mobile devices. When the mobile device tries to associate with the "known" SSID, it will encounter a different security protocol than it has remembered for that SSID. Because it cannot connect to the AP with the unknown security protocol it will continuously sending out null packets to see if the AP is still there. In that way the theory on how the Wi-Fi monitor will receive additional probe requests is explained. In practise, the performance was not improved.

The second issue was that not all mobile devices were scanned by the Wi-Fi monitor. Especially newer devices tended to be invisible in the logs. At a certain time, one of these newer devices did show up in a log of one Wi-Fi monitor but not on the other. Apparently, one of the Wi-Fi monitors had been previously updated and the other was not. After updating the Wi-Fi monitor, the newer mobile devices were scanned.

## 2.1 Implementation of the Wi-Fi Monitors

Being aware of the disadvantages of the Wi-Fi monitors, for determining the implementation of these devices the advantages are equally important. All mobile device types are detected which makes this method accessible for all users, including users of Apple devices. Also the possibility to store all the data externally on a database is a big advantage. In this way all the data can be reached from any location without the need for information from the mobile device of the user. This last advantage can be used for providing information to the museum. It has been demonstrated the direction of the movement of people can be computed and also the amount of people can be calculated by using information provided by the Wi-Fi monitors. The museum managers can retrieve this information every moment of the day from their computer, without specific information from the user.

## 3. FINGERPRINTING TECHNIQUE

Fingerprinting is a commonly used indoor localization method due to the high accuracy of location determination and low costs of implementation as it is usually possible to use (a part of) the existing infrastructure (Haojun et al., 2011). Another advantage is that this technique can have a high location calculation frequency, also called location granularity. This means that the location calculation frequency can be adjusted to what is necessary for the purpose of the indoor localization. This makes it employable for a wide range of purposes. However, there are also some important disadvantages of Wi-Fi fingerprinting. Firstly, implementation is extremely time consuming since the offline phase takes a lot of time and effort (Machaj and Brida, 2012). Secondly, fingerprinting does not work well in open spaces due to the lack of unique signal strengths in such spaces (Lu et al., 2013). Thirdly, there are many external circumstances that influence the accuracy of the localization. For example, the presence of public or using different kind of mobile devices influences the measured signal strength and thus the accuracy of the measurements (Ma et al., 2008). Finally, an important disadvantage of this technique is that Apple devices are excluded from this localization method because they are not able to carry out a Wi-Fi scan since all such sniffer applications are banned (WlanBook, 2013). Fingerprinting is based on comparing the unique signal data from a source send at a particular location with a radio map of data (Fallah et al., 2012). Localization based on fingerprinting technique includes two phases, an offline phase and online phase. The offline or training phase is about collecting the data for the radio map and in that way obtaining a unique signature of signal strengths of different access points at multiple locations at the research area. The online phase includes the comparison of the received signal strength values to the radio map and in that way give the approximate location of the user (Rehim, 2004).

### 3.1 Theory

In this research a Wi-Fi fingerprinting application created in the Wuhan University was used. This application makes use of the Parametric Signal Strength Distributions for location determination described by Rehim (2004). As it has already been stated, the process consists of two phases, the offline and online phase.

In the offline phase a radio map is created, signal strengths of the present access points are measured and processed. It is assumed that the signal strength is normally distributed. The location of the various access points is unknown, which reduces the problem to defining the parametric distribution fitting the signal strength as if it would come from a single access point. The parametric distribution is defined by calculating the probability density function (pdf) of the Gaussian distribution.

In the online phase the users measurement (signal strengths  $s$ ) is compared to the previously created radio map and a location  $x$  with the highest probability  $P$  is selected and returned. To find the highest probability of certain signal strengths at a certain location, once again the Gaussian distribution is used (Rehim, 2004).

#### 4. WI-FI MONITORED FINGERPRINTING.

"Fingerprinting techniques are especially appropriate for the range of frequencies in which GSM and Wi-Fi networks operate (approx. 850 MHz to 2.4 GHz) because of two main reasons: the signal strength at those frequencies presents an important spatial variability, and also a reliably consistency in time (despite the variable nature of radio signals)" (Martin et al., 2010). Additionally, the authors state that the fingerprinting methods already proved to be able to deliver better accuracies compared to propagation-based methods. An attempt has been made for localization with only two Wi-Fi monitors. The Wi-Fi monitors were already taken into account in the WLAN-infrastructure in the fingerprinting method for the DaRen application. Therefore the data needed for fingerprinting is already present in the database of the Wi-Fi monitors.

Similar as with normal fingerprinting an offline phase is needed to create the radio map. All the reference points are already measured for the actual fingerprinting method of the DaRen application, however a radio map has to be created. The RSSI measured by both Wi-Fi monitors for every reference point is required to create a radio map of this method. The exact time of every measured reference point is known, which is at least 4 minutes, including the MAC-address of the mobile device that was used for measurement. A query in the database can filter the data, so that the different RSSI values remain for the given reference point and Wi-Fi monitor. The averages of these values are taken into account. This has been done for every reference point for both monitors until a table is created with X, Y and RSSI thus creating the radio map.

##### 4.1 Comparison.

There are some advantages and disadvantages of the method as compared to the original fingerprinting which are discussed below:

1. The advantage of Wi-Fi monitoring fingerprinting stems from the fact that no additional application is required to scan the APs and derive the RSSI. On the other hand, Wi-Fi monitors are more expensive than the regular APs used for original fingerprinting.
2. Additional advantage is that all the data is stored directly in the database. The data is accessible every moment of the day and in thus can provide real-time information to the museum. Adding additional Wi-Fi monitors will enrich the information provided thus improving the quality. Furthermore, when the data is stored in the database, it is possible to provide information to the user about the location of other people thus enabling him to avoid crowded exhibits. This also includes

people who are not using the application, but who only have their Wi-Fi enabled on their mobile device. On the other hand, the downside of storing data in the database related to privacy issues as users should give permission to let the application use their location for different purposes.

3. The interval between two consecutive scans with the Wi-Fi monitors is relatively big and a smaller interval is required for localization. Visitors of the museums tend to walk slow and therefore give the Wi-Fi monitors the opportunity to scan the users while they are still in the same place. However, this is not a suitable for localization purposes.

4. Besides the differences in method, there is also a difference in signal strength. A comparison has been made between the signal strengths measured by the Wi-Fi monitors and measured by the mobile device. Measurements are used from both devices scanning each other at the same time. A conversion for the signal strength from the mobile device is necessary. The mobile device measures in dBm, while the Wi-Fi monitor measures quality in percentage where the dBm is between -90 and -40.

#### 5. PRIVACY ISSUES

The 3D indoor navigation system DaRen falls in the category of location-based services (LBS). LBS uses the user location to deliver a service. Privacy is a serious issue for LBS and it can have a great impact on the success of these services. An example of this, are the recycling bins of the company Renew (Dato, 2013). This company installed recycling bins with screens in the city of London that can show advertisements to people that are close. In some of these bins Renew has installed tracking devices to detect and track mobile devices, so that the advertisements to be personalised for each mobile device. The problem with this system was that MAC-addresses are tracked without the consent of the user and therefore the tracking system in the bins was not allowed by the city of London.

Besides the legal concerns, there are also the user's concerns about their privacy, such as who receives this location information, for which purpose and for how long is it used and stored (Xu et al., 2009). For DaRen project, it is important to investigate both legal and user concerns so that users' privacy to be protected. So, that then these concerns can be taken care off in the system, if they apply. In this section, first privacy is discussed where both user concerns and legal concerns are addressed. After that, it is investigated whether these concerns are applicable for the DaRen project and if these concerns are applicable how these concerns should be taken care off.

##### 5.1 Privacy

Often, privacy is described as the right to be left alone (Warren and Brandeis, 1890). This right is also been recognized by the United Nations as a fundamental right in The UN Universal Declaration of Human Rights (Loenen and de Jong, 2007). There are different kinds of privacy. In this case information privacy, in which information is regarded as personal data, is of interest. Personal data is regulated by the privacy laws of each country.

##### 5.2 User concerns

Lot of research concerning the privacy concerns of users using a LBS has been conducted. Those studies reveal that users are concerned about loss of privacy when using LBS (Xu et al., 2009). The different concerns can be categorized in four groups:

collection, unauthorized secondary use, errors and improper access. Collection reflects the concern about the extensive amount of personally identifiable data collected and stored in databases. Secondly, unauthorized secondary use is about the concern that information is collected from individuals for one purpose but is used for another secondary use without consent. Errors reflect the concern that protection against deliberate and accidental errors in personal data is inadequate. Improper access is the concern that data about individuals are readily available to people not properly authorized view or work with data. The abovementioned concerns should be considered in the design and implementation of the application. Especially the proper communication of privacy issues related to the application should be of primary importance. Users should be aware that their privacy is protected.

### 5.3 Legal Concerns

In many countries the privacy concerns are addressed by applying regulation. This means that regulations can differ per country. Therefore, in this subsection the current legislation current legislation regarding protection of privacy in the Netherlands and China are investigated.

#### 5.3.1 Netherlands.

According to the Dutch law information is personal when it can identify or has a possibility to identify a specific person. If information is personal, regulations should be applied on this information as described in the "*Wet Bescherming Persoonsgegevens*" (WBP, 2011). According to this law the user should give prior consent in order for his personal information to be used. Furthermore, it should be stated which information is used and for what purpose. Also, it is not allowed this information to be later used for other purposes or to be sold to a third party without consent. Finally, personal information is only stored till the point that information does not serve its purpose anymore and the stored information should be sufficient protected to prevent people from gaining unauthorized access. Further, this year the Article 29-working group (Article 29 Working Party, 2013) which are the privacy supervisors for the European Union gave their opinion on the area of privacy and mobile applications/LBS. They provide mobile application developers with some obligations and recommendations. Most of the obligations are more-or-less implemented in the Dutch Law. On the other hand, the recommendations such as informing the public when there is a data leak and use in the privacy condition information special for European users, are more interesting.

#### 5.3.2 China.

In China there is currently no specific legislation for protecting personal information. Only a guide of personal information protection was published in November 2012 (Shi, 2012), which became a national standard since February 2013 (Zhang, 2013). This guide divides the personal information into personal general information and personal sensitive information. The personal sensitive information is the information that can lead to harmful effect on the person when it is revealed or changed, such as the ID number, phone number and fingerprint. The personal general information is all other personal information excluding sensitive information. According to this definition, the writer thinks the anonymous personal location information belongs to the personal general information, which is allowed to be collected and processed under tacit or expressed consent of

the information source. That means that if the person does not explicitly express his or her dissent on being tracked, then his or her location can be recorded and used.

### 5.4 Privacy concerns DaRen

The first step is to identify the occurrence of personal information in the DaRen system in order to find out if data protection regulation has to be applied on the system. Since the main difference in the privacy regulation of the Netherlands and China is that the in the Netherlands the implementation is regulated by law while the substance is more-or-less the same, the Dutch privacy regulation is used to detect the occurrence of personal information. As it has already mentioned, according to the Dutch law information is personal when it can identify or has a possibility to identify a specific person. Normally in LBS during the localization or tracking of a mobile device, personal information is collected as the MAC address of the device is scanned. In DaRen project the user does not have to provide any personal information while using the mobile phone application. However, the localization component includes two sub-systems. The subsystem that provide the museum visitors' location in the application does not make use of the MAC address but the sub-system that provides the information to the museum managers makes use of it and therefore the data falls under the data protection regulation. In case that the two subsystems will be integrated into one, the implementation of privacy terms and conditions would be indisputable. The application should ask for the user's permission before being installed on the device and the purpose of collecting the MAC address of the device should be clearly stated. Moreover, personal data should be sufficiently protected from unauthorized use.

## 6. CONCLUSIONS

This paper gave insight on WiFi smartphone monitoring with respect to the WiFi fingerprinting method for the purpose of a 3D indoor navigation system. The advantages and disadvantages of both systems were listed and a conclusion is made based on the arguments given in this paper and the real-life problems that were encountered during the creation of a 3D indoor navigation application for the Hubei Provincial Museum.

## ACKNOWLEDGEMENTS

This paper is based on the work conducted by the students of the MSc Geomatics Delft University of Technology (the Netherlands) during their Syntheses Project 2013 in cooperation with LIESMARS Wuhan University (China). The project focussed on demonstrating the potential of 3D indoor navigation systems and raising awareness of the possibilities provided by the technology for every-day users. DaRen, the final product of the project is a 3D indoor navigation system for Hubei Provincial Museum (China). The synthesis project took seven weeks and was subdivided into three development phases: preparation, implementation and synthesis. The full report with test results is to be accessed from: [www.geomatics.tudelft.nl](http://www.geomatics.tudelft.nl).

## REFERENCES

- Cisco, 2013. White Paper: Presence Analytics [pdf] Cisco Meraki.  
[https://meraki.cisco.com/lib/pdf/meraki\\_whitepaper\\_presence.pdf](https://meraki.cisco.com/lib/pdf/meraki_whitepaper_presence.pdf) [Accessed 25 October 2013].

- Fallah, N., Apostolopoulos, I., Bekris, K., and Folmer, E., 2013. Indoor Human Navigation Systems: A Survey. *Interacting with Computers*, 25.1: 21-33. <http://qz.com/112873/this-recycling-bin-is-following-you/>
- Haojun, A., Taizhou, L., Jianjian, W., Menglei, Z., 2013. A New Wi-Fi Fingerprint Indoor Localization Method for Smart Phone's Heterogeneity. School of Computer Science, Wuhan University.
- Libelium, 2013. Meshlium Technical Guide v4.0 [pdf] Libelium. Available at: <http://www.libelium.com/development/Meshlium/documentation/Meshlium-technical-guide/> [Accessed 25 October 2013].
- Lu, B., Niu, J., Juny, J., Cheng, L., Guy Y., 2013. WiFi Fingerprint Localization in Open Space. State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China and Singapore University of Technology and Design, Singapore
- Ma, J., Li, X., Tao, X., and LU, J., 2008. Cluster Filtered KNN: A WLAN-Based Indoor Positioning Scheme. State Key Laboratory for Novel Software Technology
- Machaj, J., Brida, P., 2012. Impact of Radio Fingerprints Processing on Localization Accuracy of Fingerprinting Algorithms. *Electronics and electrical engineering*. No7 vol . 123
- Musa, A.B.M., Eriksson, J., 2012. Tracking Unmodified Smartphones Using Wi-Fi Monitors.
- Rehim, M.A.A.Y.A., 2004. Horus: A WLAN-Based Indoor Location Determination System.
- Shi, J., 2012. The personal information protection legislation under Web environment. Available at: [http://d.g.wanfangdata.com.cn/Periodical\\_szdxxb-zxshkxb201206013.aspx](http://d.g.wanfangdata.com.cn/Periodical_szdxxb-zxshkxb201206013.aspx)
- Sidiropoulos, N., Mioduszewski, M., Oljasz, P., Schaap, E., 2012. Open Wifi SSID Broadcastvulnerability.
- Van Loenen, B., de Jong, J., 2007. 'SDIs and Privacy: Conflicting Interests of the Spatially Enabled Society', Chapter 21, In A. Rajabifard (ed.), *Towards a Spatially Enabled Society*, ISBN 978-0-7325-1620-8, University of Melbourne, pp. 271-284
- Warren, S. D., & Brandeis, L. D., 1890. The right to privacy. *Harvard law review*,4(5), 193-220.
- Xu, H., Gupta, S., & Shi, P., 2009. Balancing User Privacy Concerns in the Adoption of Location-Based Services: An Empirical Analysis across Pull-Based and Push-Based Applications. *iConference (iSociety: Research, Education, and Engagement*, University of NorthCarolina-Chapel Hill.
- Zhang, Y., Chen, X., Jiang, J., 2010. Wayfinding-Oriented Design for Passenger Guidance Signs in Large-Scale Transit Center in China. *Transportation Research Record: Journal of the Transportation Research Board*, No. 2144, Transportation Research Board of the National Academies, Washington, D.C., 2010, pp. 150–160.

#### Websites:

Datoo, S. (2013), This recycling bin is following you.