2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 4-7 October 2016, Alcalá de Henares, Spain

Wi-Fi probes as digital crumbs for crowd localisation

Francesco Potortì*, Antonino Crivello*†, Michele Girolami*
{potorti, antonino.crivello, girolami}@isti.cnr.it
†Department of Information Engineering and Mathematics, University of Siena, Italy

Emilia Traficante+, Paolo Barsocchi*
+Cloud4Wi, Pisa
*CNR-ISTI, Pisa, Italy
etraficante@Cloud4Wi.com, paolo.barsocchi@isti.cnr.it

***Abstract*— While indoor localization techniques based on Wi-Fi RSS measurements have been extensively studied, their application to eavesdropping Wi-Fi probe requests sent from mobile devices in large indoor environments, such as shopping malls, is scarce or absent in the literature. The idea behind this work is to observe Wi-Fi enabled smartphones, especially when they are not associated to a network. They periodically perform active network scanning by issuing probe requests, which are detected by networked sniffing devices produced by Cloud4Wi®. We experimentally investigate the opportunities offered by passive gathering of Wi-Fi probes for purposes of crowd positioning in areas of interest. Our preliminary experimental setting convincingly shows that a small number of sniffing devices may be enough for analysing crowd movements in indoor areas.**

Keywords—Passive indoor localization; crowd sensing; Wi-Fi probe eavesdropping; Wi-Fi fingerprinting

I. INTRODUCTION

Network detection activities like Wi-Fi active probing or Bluetooth beaconing are regularly issued by most of the worn or pocket devices we bring with us. Such activities have the effect of disseminating digital crumbs in the network, which are usually discarded by networking devices. However, such crumbs hide a great potential for revealing interesting aspects of human behaviour, such as mobility of people in their social context.

We are interested in analysing Wi-Fi probe request messages (in the following also referred to as probes), which are issued by most mobile devices, with the goal of estimating their position. Typically, a device emits a probe every time it requires discovering the existence of Wi-Fi access points. This procedure is called *active* scan, in contrast with *passive* scans during which devices passively listen for Wi-Fi beacons from access points.

To this end Cloud4Wi (*the industry's leader in service platforms for advanced guest Wi-Fi,* http://cloud4wi.com/) leader in service platforms for advanced guest Wi-Fi, deployed a number of sniffing devices in an indoor environment, called FogSense. FogSenses passively collected a data set of probes sent by stationary and mobile devices for approximately 70 days. The environment used for the experiment is located at the Italian National Council of Research, Pisa, Italy; it covers 336 m^2 and is composed of 12 office rooms, where about 25 people work. In this paper, we analyse the data set to extract information useful to understanding the quality of the probes gathered. Specifically, we analyse the number and the distribution of probes along with the time as well as the distribution of the RSSI of the probes. We also present some useful statistics describing how well the data set captures the periodic activity of people. The goal of the analysis is to assess the potential of Wi-Fi probes to reveal useful information for crowd localization purposes.

The experimental data set is then used to apply some indoor localization techniques, in order to investigate the possibility of localizing a device using only the probes it sends. Our goal is not tracking the position of a mobile device along the time, nor identifying a specific device, rather is it to estimate *crowded* regions, i.e. areas where several devices are located for some time. Information on crowded regions can be used for several purposes, among which security, for identifying which areas should be evacuated first; marketing, for spotting areas where people gather or spend more time and are consequently more valuable; management building, to identify bottlenecks in corridors and other programmed paths. Usually, the RSS-based localization techniques can be divided into range-based and range-free methods. Range-based techniques estimate a user's position by considering the received signal strength of that user's device and exploiting a Wi-Fi signal propagation model. They are prone to errors due to reflection of waves over the walls, floor and ceiling, especially in the presence of obstacles obstructing line of sight between transmitter and receiver. On the other hand, range-free methods do not rely on the radio propagation properties of the environment. Of these, the most used is based on fingerprinting, which is based on RSS measurements made at a series of known significant points in the environment. Fingerprint methods have been studied intensively for years with remarkable and strong results in terms of localization error. For example, all competitors in the 2015 edition of the IPIN competition [16] used some form of fingerprinting, some of them exclusively so [11, 12, 13, 14, 15].

Following this trend, we experiment with three range-free algorithms, which we name Strongest, Coslinear and Combined, the latter being a combination of the previous ones. Strongest localizes a device in the same position as the FogSense receiving a probe with the highest RSS, while Coslinear is a fingerprint-based technique. The fingerprinting database is obtained by applying a linear interpolation strategy, which increases the number of fingerprint points in the database. Combined is a linear combination of the positions estimated by the previous methods.

Usually fingerprinting requires a time-consuming measurement campaign: the environment is surveyed to select the interesting locations where to gather the RSS of Wi-Fi

978-1-5090-2425-4/16/$31.00 ©2016 IEEE

networks. The operator is generally equipped with a mobile device scanning the network in an active way. In order to be reliable, this procedure is repeated at different times and with different body orientations in order to account for the signal attenuation due to the human presence, and should be periodically updated to account for changes in the environment, such as position changes of access points, furniture renovation and the such.

From an installation perspective, Cloud4Wi clients appreciate the short installation time and not having to make upgrades to existing infrastructures. To accommodate these needs, we take a different approach, by exploiting the probes the FogSenses themselves occasionally send when connecting to a central server via Wi-Fi. In fact, we build the database by recording probes sent by each FogSense and detected by other FogSenses once they are deployed in the environment. The advantage of our approach is twofold. First, we can build and rebuild the fingerprint database without any human intervention, and without any extra cost; second, we can extend our sensing architecture by increasing the number of FogSenses without any manual reconfiguration other than registering the location coordinates of new FogSenses.

The results we obtain show that the approach we follow is solid, the results are consistent and, once the method is tested and refined in a realistic environment, it can constitute a low-cost, state-of-the-art addition to Cloud4Wi's commercial offering. The remainder of the paper is as follows: Section II presents the related work; Section III describes the architecture we designed for gathering Wi-Fi probes; Section IV analyses the data set obtained, Section V presents the localization techniques we used and the measured performance. Section VI concludes the paper with a discussion about the opportunities arising from the use of probe messages as well as some takeaways.

II. Related Work

Analysis of Wi-Fi probes is gaining attention both from researchers and the industry [1,2,3]. In recent years, several techniques have been proposed to extract useful information from the probe the messages.

The author of [10] describes an experimental study showing several factors that influence the number and the frequency of the probes sent by the most popular smartphones. There are two major factors determining the behaviour of devices, namely the Operating System (OS) and the existence of known Wi-Fi networks. The author analyses some of the most recent OS by measuring the number of probes sent. As an example, devices based on Android 5.0.1 emit about 1500 probes per hour in general, while for iOS devices (IOs 8.1.3) the number of probes captured is 120 per hour. Devices usually send bursts of probes, the frequency of bursts strongly depends on the existence of known networks. We observe frequency of bursts ranging from one ever 66 s (Android 5.0.1) to one every 330 s (iOS 8.1.3).

Authors in [4] have organized a wide gathering camping with the goal of building and then analysing the social graph of the users. The authors built a social graph of the users by assuming a link between a pair of users when a similarity measure based on the Adamic-Adar metric exceeds a given threshold. Similarity is computed on the Preferred Network List provided in the probes issued by the devices, under the assumption that users that have recently seen the same access points are somehow related. The work presented in [5] exploits Wi-Fi probes to estimate the trajectory of devices. The data set is obtained by monitoring an arterial road 2.8 km long. The authors compare their solution with respect to the GPS ground-truth. Authors in [6] exploit the Wi-Fi probe messages for localization purposes. The data set refers to one of the main street of Sydney with 6 sniffing devices. They use a range-based localization algorithm.

Works presented in [7, 8] are focused on some security aspects. Specifically, [7] investigates the possibility of recognizing Wi-Fi devices by analysing certain features of Wi-Fi network drivers. Some of the features analysed by the authors are obtained by capturing Wi-Fi probes. Analogously, the work presented in [8] describes a method to recognize devices in a Wi-Fi network; the authors show that devices are recognizable even if they change their user-set name by analysing their probe messages.

Finally, the paper presented in [9] exploits the information that can be extracted from probes in order to infer insights of the relationships among users. The authors infer the user's relationships by analysing three elements: the SSIDs previously accessed by devices, a correlation of user's location and time and the frequency of co-location of devices. The user location is approximated with the location of the access point that senses a probe with the highest RSS.

All in all, to the best of our knowledge there is no direct comparison for our work in the literature and no measurement campaigns, whether extensive or not, has been published on the positioning accuracy that one can obtain by eavesdropping Wi-Fi probe request packets using sniffing devices or otherwise.

III. Probe Sniffing Architecture

Devices with an enabled Wi-Fi network periodically emit Wi-Fi probe requests. Their purpose is to actively scan the network searching for available Wi-Fi access points or for a previously accessed access point. This discovery phase usually prepares an association phase through which a device establishes a connection to a specific network.

The frequency of the probes sent by devices varies according to several factors, and depends on the driver of the Wi-Fi network and decisions made by the operating system. For example, some devices do not perform any Wi-Fi scanning when connected to a network, wired or otherwise. Our experiments showed different behaviours of Wi-Fi devices: we observed that some mobile devices probe regularly with intervals ranging from 15 to 60 seconds, while others probe with a much longer intervals ranging between 60 and 180 minutes.

We collect the probes emitted by Wi-Fi-enabled devices by means of a network of sniffing devices, namely FogSense devices distributed by Cloud4Wi®, Inc. A FogSense is a plug-and-play Wi-Fi sensor that doesn't require any calibration or time consuming set-up phase. Figure 1 shows a FogSense Wi-Fi sensor.

Fig. 1. A FogSense Wi-Fi sensor.

Every FogSense is provisioned with a USB port as well as a mini-USB port for configuration purposes. The Wi-Fi module is a Broadcom's WICEDTM from USI, supporting IEEE 802.11 b/g/n Wi-Fi standards with an operational frequency ranging from 2.402 to 2.484 GHz.

A FogSense detects the presence of nearby Wi-Fi-enabled devices and transmits the data collected to a server, which, in turn, stores the information into a database as shown in Figure 2. Data collected by the probes are periodically sent to a server in batches with a configurable interval, currently set to 15 s. Data sent includes the following information extracted from the captured probes:

- Reception time stamp
- MAC address of the sending device
- RSS (dBm) measured by the FogSense.

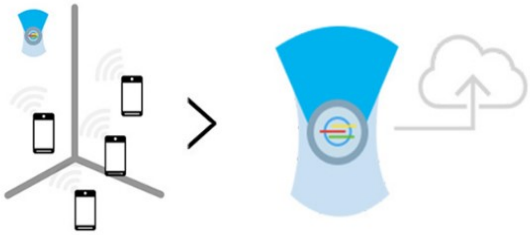

Fig. 2. Life-cycle of the FogSense.

We deploy a set of FogSenses within one of the building's wings of the Italian National Council of Research[1] (CNR), located in Pisa. The map of the sensing region we chose is shown in Figure 3.

The sensing region covers 336 m^2 and it is characterized by a straight corridor with offices located on both sides. The sensing region is made of 12 offices separated with gasbeton walls. Offices are all different sizes, including small (1 person), medium (2 people) and large offices (3 to 4 people) of respectively 10, 22, and 25 m^2. We identify 12 points of interest where to deploy the FogSenses marked with blue dots in Figure 3.

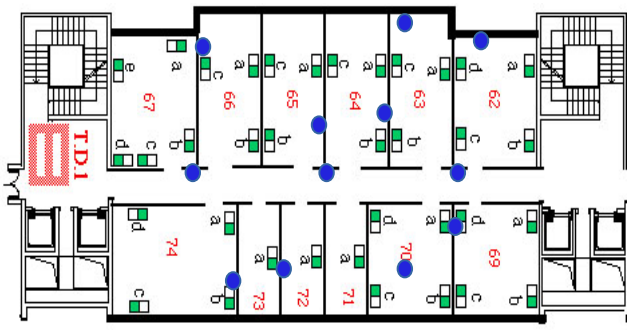

Fig. 3. Map of the sensing region. FogSenses are indicated with blue dots (green and blue squares represent the desks).

IV. Analysis of the Data Set

The data gathering campaign covers approximately 70 days from 4 March 2016. We gathered about 6 million probes and we detected over 30 thousand unique MAC addresses during the observation time. Among all the devices detected, 17 are *known* devices, e.g. workstations, laptops, smart phones and other kinds of instrumentations installed in our laboratory. All the analysis work is done on an anonymized copy of the database.

Figure 4 shows ranking of the known devices according to the number of probes they send. The two more talkative devices are two laptops (Asus and Lenovo) usually connected to a wired network whose Wi-Fi interface is enabled but not associated to any network.

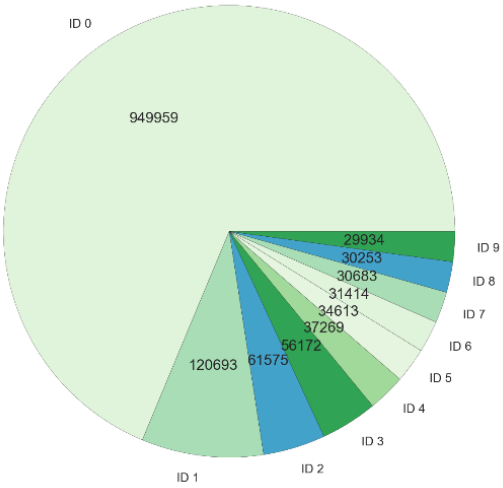

Fig. 4. Top 10 known devices by number of probes sent.

Figure 5 shows the top overall devices (known and unknown), i.e. those from which we receive the highest number of probes. We capture about 600.000 probes from each of the two most active devices. Device with ID 0 is not among the known devices, while ID 1 is our Nexus laptop.

[1] Coordinates: (43.7186389,10.4218262)

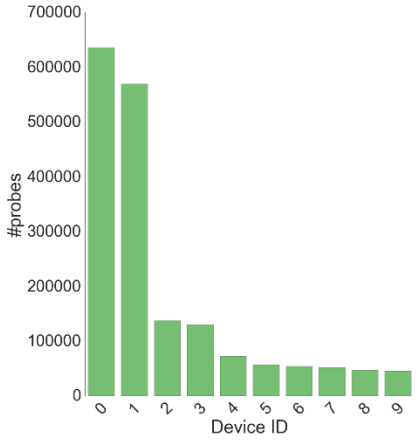

Fig. 5. Overall top 10 devices by number of probes sent.

Figure 6 illustrates the RSS distribution for all devices and for the known devices only. A small number of probes exhibit low RSS in the range of [-100, -85] dBm. These probes are probably sent from devices far from the FogSenses. On the other side, the probability distributions of the known devices better resemble the expected bell shape.

Figure 7 shows the number of probes received in 25 minute intervals as time series covering one week's time starting on 11 April 2016 in three graphs:

- *all devices* which reports the probes sent by unknown, known and FogSense devices;
- *FogSense and Known devices* which only reports the probes sent by the FogSenses and by the known devices;
- *Known devices* which shows only the probes sent by the known devices. Note the scale change.

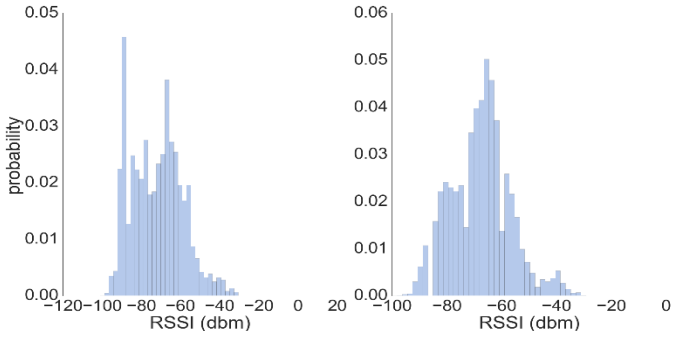

Fig. 6. Probability distribution of measured RSS values

As expected, when we consider all the devices then the number of probes is far higher than that of the probes received from the known devices. During the week depicted in the third graph of Figure 7, we collected a total of about 700.000 probes, of which about 80.000 are sent by known devices, It is especially apparent how the number of captured probes increases during the working hours and drops down during off-work hours and weekends. The trend of the captured probes shows the capability of the data set to reproduce the working rhythm of employees. The probes collected during the off-work hours and weekends are sent by stationary devices such as Wi-Fi enabled PCs.

V. Localizing Through Wi-Fi Probes

A. The Fingerprint Database

Usually, building a fingerprint database starts with selecting several calibration points. The RSS values associated with each

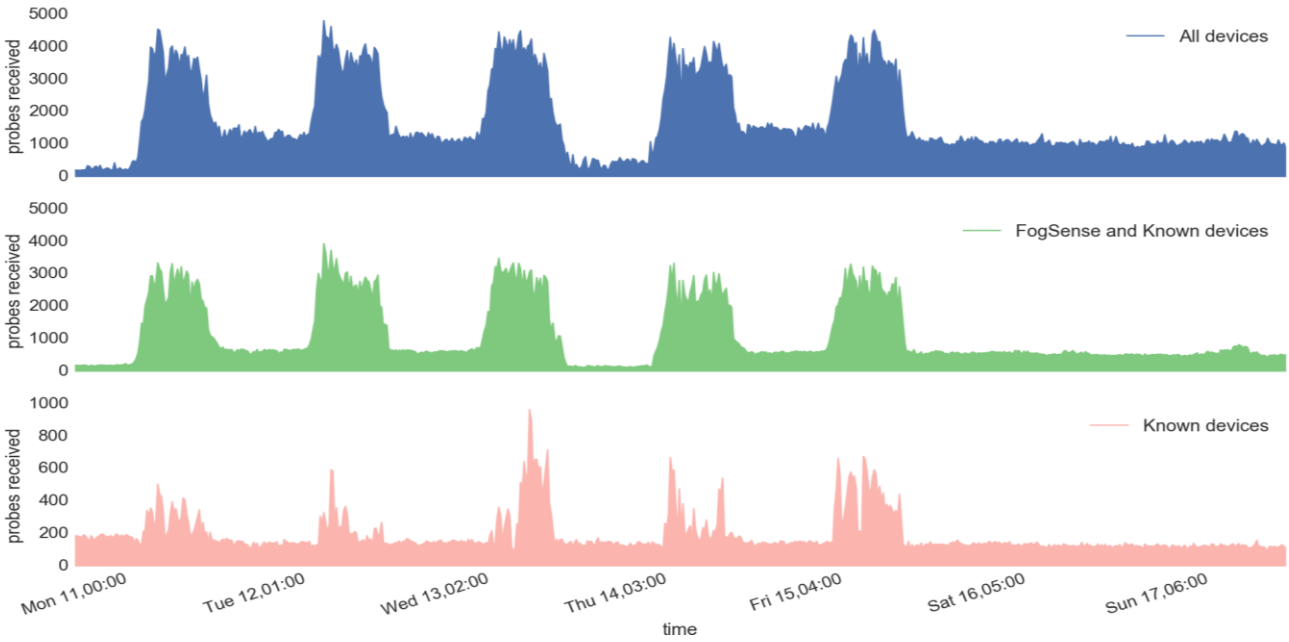

Fig. 7. Time series of probes. Note the scale change in the third graph.

access point are collected at the calibration points over a certain period of time and then stored in fingerprint database together with the location coordinates. During the operational phase the person, or object of interest, is located by comparing its observed fingerprint to those stored in the database, looking for the most similar ones. Building a working fingerprint database is definitely a time-consuming task, especially for large areas, where it may contain thousands of calibration samples.

In order to be commercially viable, the proposed method should require very little or no installation and maintenance measurements. We profit from the probes sent by the installed FogSenses themselves, which are connected via Wi-Fi to a server, and therefore occasionally send a probe request, which is collected by the other FogSenses. This is enough to build a self-updating database composed of fingerprints relative to the positions of the FogSenses. When the density of FogSenses in the environment is low, however the illustrated procedure may not be enough for reaching a satisfying positioning accuracy. We then resort to interpolation on a square grid, a method already proposed in the literature [18]. Since this is a preliminary study, we started with a very simple interpolation method, based on linear interpolation over a Delaunay triangulation whose vertices are the FogSense positions. The interpolation thus obtained covers an area corresponding to the convex hull of the FogSense position, as shown in Figure 8. This is one of the simplest possible scattered data interpolation methods, which in a further will be compared with more advanced methods, such as Kriging or the inverse-distance method.

By interpolating the measured cross-FogSense fingerprint, we obtain an interpolated set of fingerprints over the regular grid, which contributes to the database. Figure 9 shows the created RSS radio map as seen by each FogSense: this is obtained for illustrating purposes by using a grid width of 10 cm. During the localization phase, the fingerprint of the probe request sent by a mobile phone is compared with the RSS values stored in the database.

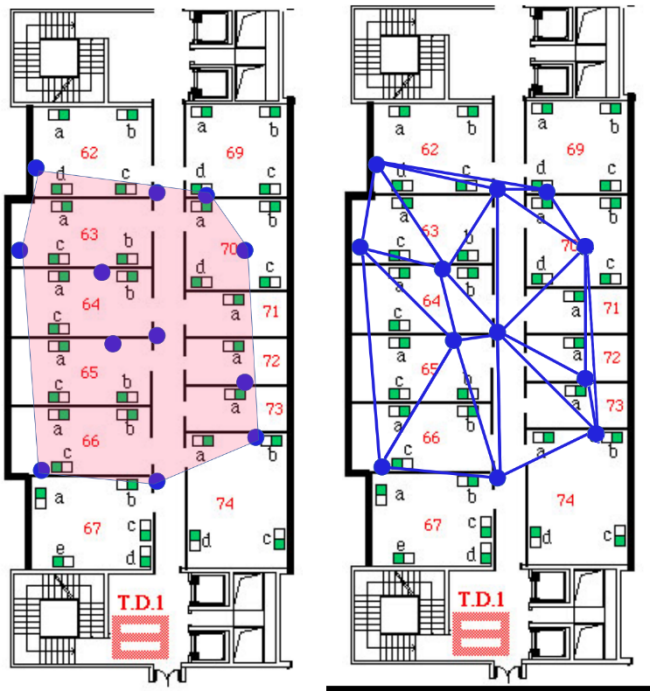

Fig. 8. Position of FogSense and Delaunay triangulation (green and blue squares represent the desks).

B. *Localization Algorithms*

We implement two algorithms, a very simple one without fingerprinting, and the other based on interpolated fingerprinting. Both us *k*-NN. A third method is a combination of these two.

k-NN is a supervised learning algorithm where new objects are classified based on a voting criteria: the *k* nearest objects from the training set are considered, and the new objects are assigned the class of the majority of those. In fingerprinting

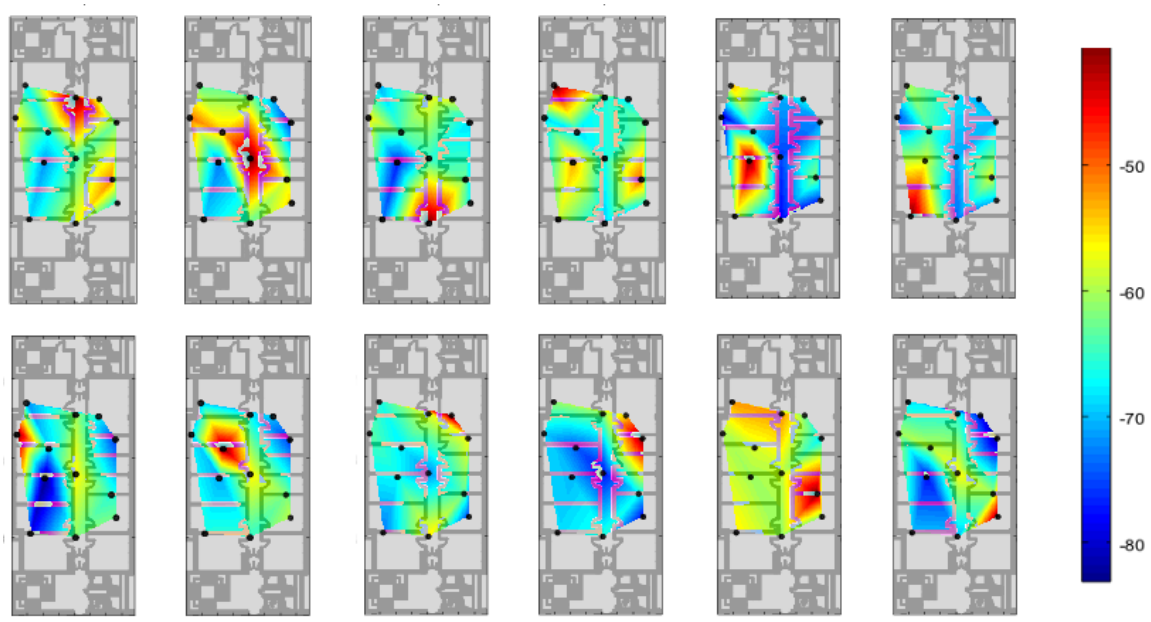

Fig. 9. The RSS radio map built for every FogSense deployed.

localization methods, the position of the person is chosen by assigning the location where the RSS values are the most *similar* among those of the k samples stored in the database. In the simplest instance, the centroid of positions of the k fingerprints in the database is considered.

The simpler algorithm, named ***Strongest***, it takes as estimated positions those of the k FogSenses whose RSS values is highest in the fingerprint.

The interpolated fingerprint algorithm, named ***Coslinear***, uses a cosine similarity measure, and then considers the k nearest fingerprints in the database. The cosine distance between two vectors A and B is defined as:

$$CosDistance(A,B) = 1 - \frac{A * B}{||A|| * ||B||}$$

We chose the cosine similarity because, for our data set, it performs better in terms of localisation error, than the other similarity measures we experimented with. Specifically we tried p-norms with $p = 1$ (Manhattan distance), $p = 2$ (Euclidean distance), $p = \pm\infty$ (compare only max or min abs values). All the p-norms used where considered in two different flavours: using straight RSS values, and using differential RSS values, in order to remove the bias given by different devices possibly sending probes with different transmitting power.

By interpolating the measured cross-FogSense fingerprint, we obtain an interpolated set of fingerprints over the regular grid, which contributes to the database. Figure 9 shows the created RSS radio map as seen by each FogSense: this is obtained for illustrating purposes by using a grid width of 10 cm. During the localization phase, the fingerprint of the probe request sent by a mobile phone is compared with the RSS values stored in the database.

Finally, the ***Combined*** algorithm estimates the position of a device as the midpoint of the position estimates given by the Strongest and Coslinear algorithms. The rationale of this choice is that, as detailed below, the Strongest and Coslinear algorithms give estimates of similar quality, and to an extent independently computed, their combination is expected to benefit from both.

This simple criterion is used here as a proof of concept: the idea for future work is that of using several different algorithms and combine them after studying their correlation properties.

C. Experimental Results

We consider the positions of 17 known devices to evaluate the performance of the three algorithms. All devices are Wi-Fi enabled and they are deployed all of the rooms of our sensing region. Some of the devices are laptops and workstations, most are smartphones plugged to the power line and normally kept in a fixed place on a desk. Figure 10 shows the positions of the known devices depicted as blue crosses.

Figure 11 shows the median error of the positioning estimates for some devices, where *error* is defined as the Euclidean distance from the estimated position to the position where the devices were located most of the time during the 70 days of the experiment.

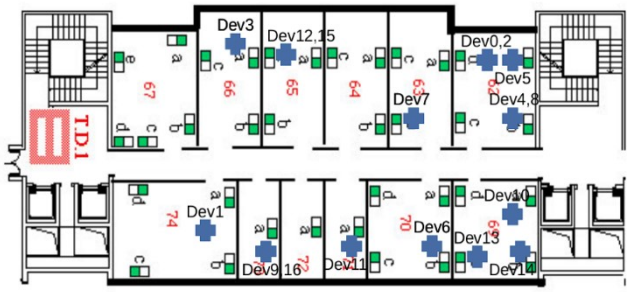

Fig. 10. Position of known devices (green and blue squares represent the desks).

Note that a more appropriate performance estimate would be the third quartile of error as used in [17], however we choose to use the median given the preliminary nature of the measurements presented here. Figure 11 depicts the median

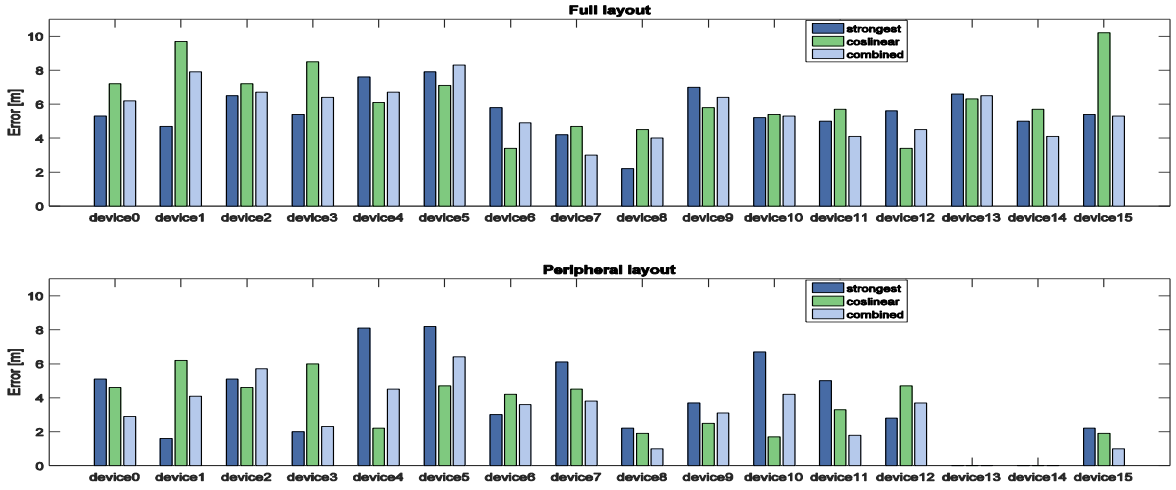

Fig. 11. Median error of the localization algorithms with 5 devices, w =4 and with full/ peripheral layouts.

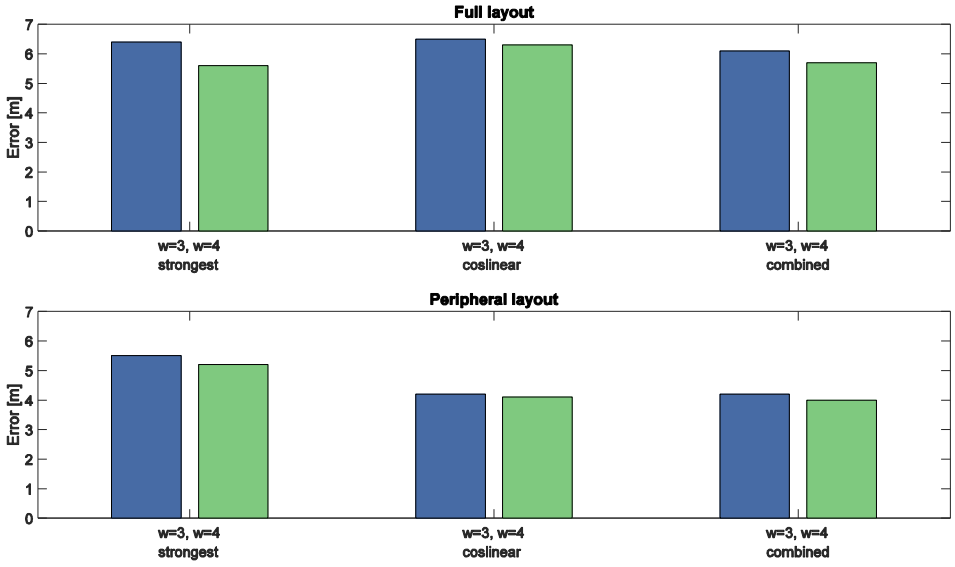

Fig. 12. Median error for the localization algorithms with all devices, w =3,4 and with full/peripheral layouts.

error for 4 combinations of parameters: *minimum fingerprint length* and *FogSense layout*. The minimum fingerprint length is included because probes sent by devices can be missed by the FogSenses, and most often fingerprints have not their full length. We considered the two cases of fingerprints of lengths $w > 2$ and $w > 3$: results are generally better with longer fingerprints. The FogSense layout indicates the subset of FogSenses used to compute the fingerprinting database: we consider two layouts of the FogSense, the full layout which considers all the deployed FogSense deployed (as shown in Figure 3), and the peripheral layout which only considers the FogSense deployed on the four corners of the area. It is interesting to note that the Coslinear method gains a little with respect to the simpler Strongest algorithm with this layout.

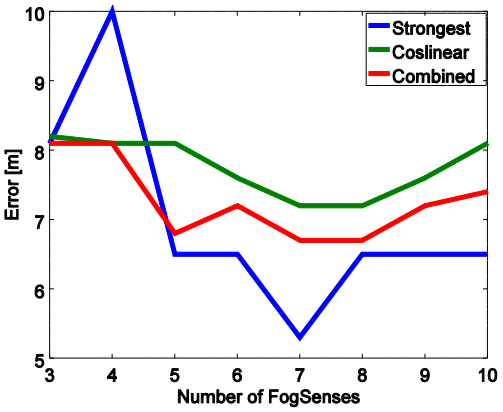

Fig. 13. Median error for all device versus number of FogSenses

As expected, the resulting accuracy varies with the devices, i.e. there are lucky and unlucky spots in the sensing region. Also, there is no clear winner between the Strongest and Coslinear algorithms, while Combined is almost never worse than the first two and sometimes is better than both, the reason likely being that the errors of the two first algorithms have little correlation. In general, the performance is quite satisfactory considering the low frequency of the probes emitted by devices, the different and often unpredictable behaviour of the devices, the packet loss, all factors which are likely to reduce the positioning accuracy. To compare these experimental results with an excellent base line, we consider the results of the EvAAL-ETRI 2015 offline competition, where the four competitors produced median errors between 4.5 and 7 m.

Figure 12 shows overall statistics on the experiment. Since the devices are very different in their behaviour, in terms of number of fogs produced, computing a single statistics on all the errors would produce skewed results. As a partial solution, we computed the average of the median errors for all devices, for the 4 combinations of parameters. Here it is more apparent how the Combined algorithm provides good results with both layouts and with both w values. Note that, as expected, for $w = 4$, the localization error tends to decrease for all the algorithms and in both layouts. The error is lower in the layout with only 4 FogSenses, indicating that apparently a high density of receiving devices does more harm than good. Moreover, the higher w advantages the Strongest algorithm more than the Coslinear one, which appears more stable for varying number of probes per fingeprint.

In order to support these observations, we computed the median of all errors for all devices considered as one, computed on many hundreds of possible subset of FogSenses having minimum distance of 4 m between them. The results are plotted in Figure 13 as median error vs. number of FogSenses, and are interesting for two reasons. First, they show a general trend of diminishing error vs. number of FogSenses up to a point, and then a rise, which seem to support the hypothesis that too high a density of receiving devices is harmful. Second, and most important, they clearly indicate that the Strongest algorithm takes the best advantage from a higher number of FogSenses, which is to be expected given the nature of the algorithm, while

the Coslinear algorithm is more robust in the face of varying number of FogSenses.

Given these observations, we are planning further experiments in bigger indoor environments, where we expect that the low density of FogSenses will strongly penalise the Strongest algorithm in favour of the Coslinear algorithm, which has promise to provide usable results even with a small number of FogSenses.

VI. Conclusion

To the best of our knowledge, the literature lacks experimental investigations on the possibility of localisation of crowds in indoor environment using passive detection of Wi-Fi probes produced by mobile devices. We set up an experimental environment and we measure the performance of localisation methods that do not require installation measurements nor maintenance.

We present a modular architecture designed to collect the Wi-Fi probes periodically emitted by Wi-Fi-enabled devices. We collect about 6 million probes emitted by mobile and stationary devices over a span of 70 days. We analyse the data set by providing some base statistics and we show the performance of three range-free localization algorithms based on the median localisation error in different conditions and with different settings.

We derive some key takeaways as well as some considerations from this experimental campaign. First, the architecture we proposed is modular, in that it is possible to extend or reduce the number of FogSenses without any architectural change. Moreover, our strategy relies on passively collecting probes emitted by devices: mobile, stationary and also the probes emitted by FogSenses. This represents a strength when it comes to building a fingerprint database, or any other data base for localisation purposes. In fact, our approach does not require to survey the environment, select the points where to gather the RSS values and finally to collect data with one or more sensing devices. We avoid all these steps by exploiting the probes sent by the FogSenses themselves. Finally, the results obtained with three different algorithms are, in our opinion, remarkable. In fact, the median errors of the algorithms tested are directly comparable with the results of some of the best localization algorithms based on Wi-Fi fingerprint presented and, most importantly, tested, during the EvAAL 2014 and EvAAL-ETRI 2015 competitions.

We claim that exploiting Wi-Fi probes promises to be a viable and cheap strategy for an indoor crowd localisation solution that monitors the positions of anonymous groups of users in a big indoor environment.

References

[1] S. Savazzi, M. Nicoli, F. Carminati, and M. Riva, “A bayesian approach to device-free localization: Modeling and experimental assessment,” Selected Topics in Signal Processing, IEEE Journal of, vol. 8, no. 1, pp. 16–29, Feb 2014.

[2] J. Wilson and N. Patwari, “Through-Wall Motion Tracking Using [Variance-Based Radio Tomography Networks,” IEEE Transactions on Mobile Computing, vol. 10, no. 5, pp. 612–621, May 2011.

[3] N. Patwari, M. Bocca, and O. Kaltiokallio, “Enhancing the accuracy of radio tomographic imaging using channel diversity,” 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012), vol. 0, pp. 254–262, 2012.

[4] M. V Barbera, A. Epasto, A. Mei, V. C. Perta, and J. Stefa, “Signals from the Crowd : Uncovering Social Relationships through Smartphone Probes,” *Conf. Internet Meas.*, pp. 265–276, 2013.

[5] A. B. M. Musa and J. Eriksson, “Tracking unmodified smartphones using wi-fi monitors,” *Proc. 10th ACM Conf. Embed. Netw. Sens. Syst. - SenSys ’12*, p. 281, 2012.

[6] Z. Xu, K. Sandrasegaran, X. Kong, X. Zhu, J. Zhao, B. Hu, and C. Lin, “Pedestrain Monitoring System using Wi-Fi Technology And RSSI Based Localization,” vol. 5, no. 4, pp. 17–34, 2013.

[7] J. Franklin, D. Mccoy, and J. Van Randwyk, “Passive Data Link Layer 802 . 11 Wireless Device Driver Fingerprinting,” pp. 167–178.

[8] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, “802.11 User Fingerprinting,” *Mob. Comput. Netw.*, p. 99, 2007.

[9] N. Cheng, P. Mohapatra, M. Cunche, M. A. Kaafar, R. Boreli, and S. Krishnamurthy, “Inferring user relationship from hidden information in WLANs,” *Proc. - IEEE Mil. Commun. Conf. MILCOM*, 2012.

[10] Julien Freudiger, “How talkative is your mobile device?: an experimental study of Wi-Fi probe requests”, *Proc*. WiSec '15., New York, USA.

[11] Y. Li, P. Zhang, X. Niu, Y. Zhuang, H. Lan and N. El-Sheimy, "Real-time indoor navigation using smartphone sensors," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-10.

[12] P. Wilk, J. Karciarz and J. Swiatek, "Indoor radio map maintenance by automatic annotation of crowdsourced Wi-Fi fingerprints," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-8.

[13] A. Moreira, M. J. Nicolau, F. Meneses and A. Costa, "Wi-Fi fingerprinting in the real world - RTLS@UM at the EvAAL competition," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-10.

[14] S. Knauth, M. Storz, H. Dastageeri, A. Koukofikis and N. A. Mähser-Hipp, "Fingerprint calibrated centroid and scalar product correlation RSSI positioning in large environments," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-6.

[15] R. Berkvens, M. Weyn and H. Peremans, "Localization performance quantification by conditional entropy," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-7.

[16] F. Potortì, P. Barsocchi, M. Girolami, J. Torres-Sospedra and R. Montoliu, "Evaluating indoor localization solutions in large environments through competitive benchmarking: The EvAAL-ETRI competition," Indoor Positioning and Indoor Navigation (IPIN), 2015 International Conference on, Banff, AB, 2015, pp. 1-10.

[17] P. Barsocchi, S. Chessa, F. Furfari and F. Potortì, "Evaluating Ambient Assisted Living Solutions: The Localization Competition," in IEEE Pervasive Computing, vol. 12, no. 4, pp. 72-79, Oct.-Dec. 2013.

[18] B. Li, Y. Wang, H. K. Lee, A. Dempster and C. Rizos, "Method for yielding a database of location fingerprints in WLAN," in IEE Proceedings - Communications, vol. 152, no. 5, pp. 580-586, 7 Oct. 2005.