Analyzing Passive Wi-Fi Fingerprinting for Privacy-Preserving Indoor-Positioning

Lorenz Schauer, Florian Dorfmeister, and Florian Wirth
Mobile and Distributed Systems Group
Ludwig-Maximilians-Universität München
Munich, Germany
Email: lorenz.schauer@ifi.lmu.de, florian.dorfmeister@ifi.lmu.de, wirthf@cip.ifi.lmu.de

***Abstract*—Wi-Fi fingerprinting is the most actively investigated indoor positioning technique, yielding adequate positioning accuracy on existing wireless infrastructures. However, the positioning process commonly requires active 802.11 scans where probe requests are sent out. These frames can easily be captured and used for tracking mobile devices without the users' consent or even awareness. In order to preserve the users' privacy, a fully passive positioning process for Wi-Fi fingerprinting is proposed in this paper. With the presented approach, a mobile device passively listens for beacon frames in monitor mode to determine a valid RSSI fingerprint while not sending out any information. Our passive method is evaluated against common active fingerprinting in a real-world environment. The obtained results yield the conclusion that the proposed approach performs even slightly better in terms of accuracy and precision. Furthermore, less time is needed for obtaining a position fix, while preserving the users' privacy during the acquisition of position updates.**

I. Introduction

The immense proliferation of modern mobile devices have led to a widespread and ubiquitous usage of Wi-Fi. Due to the vast number of deployed access points, Wi-Fi is currently seen as one of the most promising techniques for indoor positioning, as GPS is not operating inside buildings.

One of the most popular approaches in this context is Wi-Fi fingerprinting, which has first been presented in the RADAR system [1]. It basically consists of two phases: In the offline training phase the received signal strength indicators (RSSI) of all access points (AP) in reach are measured at a certain grid of reference points. The RSSI measurements and its locations are stored into a fingerprint database, the so-called radio map. In the online phase, a device performs an IEEE 802.11 active scan determining the RSSI vector of all APs in reach at the current location. This vector is compared to the radio map and the most probable position estimation is returned.

Wi-Fi fingerprinting achieves adequate positioning results, but suffers from an extensive training phase. Therefore, many investigations have focused on reducing these efforts for creating the radio map, e.g., [2], rather than on solving privacy issues. Only few works exist presenting approaches for privacy preservation in Wi-Fi fingerprinting, such as [3] or [4]. However, none of these works concentrate on the commonly used IEEE 802.11 active scanning process itself, where unencrypted management information is sent out. This information can be easily captured, and used for target tracking without the users' awareness, as shown in [5].

We concentrate on this privacy problem, and present a modification to the online phase of common Wi-Fi fingerprinting. The basic idea is to use only IEEE 802.11 passive scans in order to determine the RSSI vector. Thus, a mobile device just listens on the unsolicited beacon frames periodically sent by any AP, rather than actively sending any frames itself. Therefore, neither the provider of the radio map nor any third party within range are able to track users' movements.

Furthermore, we demonstrate that the accuracy and precision of our beacon based fingerprinting (bFP) is at least as good as of common Wi-Fi fingerprinting with active IEEE 802.11 scans, named aFP below. For this purpose, we implement bFP with a deterministic and a probabilistic approximation algorithm, using weighted kNN and Naive Bayes classifier, respectively. Both techniques are widely used in aFP systems [6]. The evaluation is based on various position fixes on a mobile device using both aFP and bFP with our office building's existing Wi-Fi infrastructure. We evaluate the system's accuracy and precision and compare the results of aFP and bFP. Furthermore, we compare bFP with the results obtained at SMARTPOS [7], a previous work on precise Wi-Fi fingerprinting by our group.

Overall, this paper is structured as follows: Section II gives a brief overview of related work. In Section III, the technical background and basic principles are introduced. Section IV presents our evaluation, and finally, Section V concludes the paper and gives hints on future work.

II. Related Work

Privacy-preserving approaches are well studied in the field of indoor positioning and wireless LANs. Jiang et al. [8] analyze the problem of location privacy in wireless infrastructures and introduce a protocol to protect the user's location. They already consider silent attackers capturing Wi-Fi packets within communication range as the strongest attackers for users' privacy. Note, that our bFP protects the positioning process against these silent sniffers.

Konstantinidis et al. [9] introduce a method for privacy-preserving indoor positioning on mobile devices. The authors propose an approach to protect users against location tracking by the localization service. However, neither the scanning

 DOI: 10.1109/ICL-GNSS.2016.7533851

procedure nor any data sent from the mobile device, such as current Wi-Fi fingerprints, are particularly protected.

Li et al. [4] propose a privacy-preserving Wi-Fi fingerprint localization scheme protecting both the data privacy of the localization service provider and the user's location. For the latter, they use the Paillier cryptosystem to realize an encrypted transmission of online fingerprints from mobile devices to the localization server. Thus, the measured RSSI vectors is then protected against sniffer attacks, but the scanning process is still active and can be captured by third persons within communication range.

Gschwandtner and Schindhelm [3] closely relate to our own investigations. They achieve privacy-preserving Wi-Fi fingerprinting using enhanced Wi-Fi beacons. All required positioning information are added into the information elements of beacon frames. Thus, the client is able to calculate its' position locally. It is also mentioned to listen on the enhanced beacon frames only, rather than sending probe requests. However, the mentioned idea is not further investigated, nor evaluated in a real-world scenario. Hence, we fill in this gap, and present a concrete implementation of a beacon based fingerprinting on a mobile phone. Furthermore, we evaluate our approach against common Wi-Fi fingerprinting methods in terms of position accuracy and precision in a real-world environment. To our knowledge, this has never been investigated before.

III. Basic Principles

A. IEEE 802.11 network discovery

Wi-Fi is defined in IEEE 802.11 [10] introducing three different frame types, such as control, data, and management frames. We focus on the latter, due to the fact that these are involved in the 802.11 network discovery procedure which can be active or passive. When performing passive scans, a client listens on beacon frames which are periodically transmitted by APs over all operating channels. Thus, the client iterates over all available channels and listens on each channel for a maximum duration defined by the *MaxChannelTime* parameter. Notice, that due to mismatching channels clients may miss transmitted beacons using this procedure.

For a more efficient network discovery, most clients prefer active scanning sending out probe requests iteratively for each channel. These frames contain unencrypted device specific information, e.g., MAC address, or destination's network name (SSID). All management frames can simply be captured by any Wi-Fi card in monitor mode. Hence, information about preferred network SSIDs and the sender's MAC-Address is easily accessible for silent attackers. Furthermore, continuous active scans in an area of interest, e.g., performed during common Wi-Fi fingerprinting, can be used to track users' trajectories [11]. In summary, Wi-Fi active scans in conjunction with indoor positioning systems lead to privacy issues. Therefore, we investigate a purely passive Wi-Fi fingerprinting based on using recorded beacon frames only.

B. Location Estimation

Location estimations based on a recent online RSSI vector can be performed in a deterministic or probabilistic manner [6]. Both variants are described for our bFP in the sequel. Furthermore, we consider the users' orientation for location estimations using the built-in accelerometer and magnetometer sensors, which are commonly integrated in mobile devices. Online RSSI measurements can then be compared to more specific database records according to the orientation. This is common practice, due to the fact that the human body may affect the location estimations [7], [12].

1) Passive Fingerprint Creation: In common Wi-Fi fingerprinting systems, the creation of the radio map is usually based on active scans. However, this procedure involves probes being sent by the user's device, which can ultimately lead to an infringement of the user's communication and location privacy. Therefore, we deploy passive fingerprint creation as follows: For a specific time interval Δt, the mobile device listens for incoming beacon frames while iterating over the possible radio channels, switching channels after another interval Δt_h. This channel hopping is necessary to capture signals from all APs in reach operating on different channels. The fingerprint vector v is filled with the mean RSSI values $\overline{v_i}$ of each AP seen. Different values of Δt impact both the duration of determining v and the amount of information contained in a single fingerprint, which may influence the position accuracy as it is able to planish the impact of an observed RSSI outlier. Hence, this parameter can be adapted to different use cases depending on constraints concerning duration and accuracy of a position fix. E.g., when a persons is moving, Δt should be much smaller than for users sitting in their office.

2) Deterministic Approach: According to SMARTPOS [7], we consider both weighted and non-weighted kNN (k-nearest neighbors) classifiers in signal space during the online phase. Based on the Euclidean distance $d_i = dist(v, r_i)$ between a passively measured RSSI vector v and a specific record r_i of the fingerprint database, we determine the k nearest candidates of possible user positions. Using non-weighted kNN classifier, the centroid of these k positions is calculated and returned to the user as current location. In addition, the weighted kNN method multiplies an individual weight w_i to each of the k position candidates, with w_i being calculated as:

$$w_i = \left(d_i \sum_{j=1}^{k} \frac{1}{d_j} \right)^{-1} \tag{1}$$

The current location estimate is then calculated as the sum of weighted k position candidates. Note, that the authors of SMARTPOS obtained better results using the weighted procedure. So, we also investigate both types of kNN classifiers for our bFP and compare the results.

Whenever an online RSSI vector is compared, it is possible that any two vectors differ in their lengths. Thus, one has to find a consistent way of dealing with missing values. Corresponding RSSI values can either simply be ignored or be set to a predefined minimum value for missing data,

which should be lower than the minimal actually measurable RSSI value [7]. When ignoring matchless entries, important information for accurate location estimations may be lost, while negative effects caused by changes occurring in the setup of access points may be kept low. On the other hand, a fixed minimum value punishes comparisons between strong RSSI and missing values, and favors comparisons between weak RSSI and missing values. However, this is to be expected in real-world scenarios where strong signals should be measured again at the corresponding position, while weak signals may be missed, due to strong fluctuations of radio signals within buildings. Notice, that SMARTPOS shows better results when ignoring missing values.

3) Probabilistic Approach: Following to SMARTPOS, a naive Bayes classifier is used. Unlike before, this approach returns a specific room number to the user. To this end, room information has to be saved together with corresponding RSSI vectors in the radio map during offline phase. More specifically, our naive Bayes classifier is based on the Bayes theorem and assigns the most probable class to a problem instance represented by a feature vector. In our case, we treat rooms as classes, and vectors of RSSI measurements as problem instances and feed them to Bayes theorem:

$$P(R|v) = \frac{P(v|R) \cdot P(R)}{P(v)} \tag{2}$$

calculating the posteriori probability $P(R|v)$ of being in a certain room R in the case fingerprint v is observed. The probability $P(R)$ is the prior probability which is based on our knowledge of frequencies in the training set, and hence, it can be easily estimated by counting the occurrence of each room. $P(v|R)$ is the likelihood function determining the probability of observing v in case of being in room R, and $P(v)$ is called the evidence which can be calculated assuming a normal distribution with mean μ and the standard deviation σ for each one-dimensional parameter.

The naive Bayes classifier is simple to use, given the fact that it always assumes conditional independent features. Hence, we are allowed to express the probability of being in a certain room R in case of observing fingerprint v consisting of n access points' (mean) RSSI values v_i as follows:

$$P(R|v_1, ..., v_n) = \frac{1}{Z} P(R) \prod_{i=1}^{n} P(v_i|R) \tag{3}$$

with evidence $Z = P(v)$ treated as a constant in this case, because the values of RSSI measurements are known. Due to the fact that the value of Z does not change, and us only being interested in the most probable room R_j with $j \in 1, ..., |R|$ using the maximum-a-posteriori (MAP) decision rule, the naive Bayesian classifier can be directly derived from Equation 3 and is expressed as follows:

$$R = \underset{R_j}{\operatorname{argmax}} \{P(R_j) \prod_{i=1}^{n} P(v_i|R_j)\} \tag{4}$$

Hence, applying an online measured RSSI vector of length n to Equation 4, the most probable room R_j out of all labeled rooms R is returned by the proposed naive Bayes classifier. Note, that a similar probabilistic estimator is also used in SMARTPOS, but is not described by the authors how they treat missing values in this case.

Being linked by means of multiplication, however, observed RSSI values that are lacking their counterpart in the radio map for a certain room R_j would rigorously lead to zero-probability of R_j. In our case, this would lead to false classifications, due to the fact that a room will consequently show the probability of zero even if only one RSSI value is missing. In order to solve this problem, a small sample correction is added to all probability estimations guaranteeing that no probability is ever set to zero. These corrections are called pseudocounts or additive smoothing, which is commonly used with naive Bayes classifiers in order to treat missing values. In our case, we use Laplace smoothing for all of our measurements v_i taken in a certain room R_j and smooth $P(v_i|R_j)$ with a pseudocount $\gamma = 1$. This is done according to the following Equation:

$$\hat{P}(v_i|R_j) = \frac{\text{count}(v_i)_{R_j} + \gamma}{|v|_{R_j} + \gamma \cdot (v)_{R_j}} \tag{5}$$

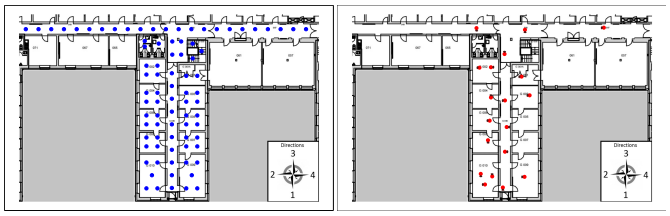
where $\text{count}(v_i)_{R_j}$ is the number of occurrences of the measurement v_i in room R_j, $|v|_{R_j}$ is the amount of all measurements made in room R_j, and $(v)_{R_j}$ is the domain of all measurements observed in room R_j. By using this Laplace smoothing technique, we are able to consider all of our rooms for classification even when our measurement data differ from the corresponding entries in the radio map. Thus, Equation 4 is still correct for the whole set of possible rooms and returns the most probable room.

IV. Evaluation

Our approach is evaluated using the existing wireless infrastructure in our institute's office environment. The results are compared to common active Wi-Fi fingerprinting in terms of well-known performance criteria, which are also used by SMARTPOS. We analyze the mean, minimum and maximum positioning errors as well as the standard deviation using different values of k. Furthermore, we investigate the impact of different factors on the performance of our approach, i.e., consideration of the user's orientation, usage of weighted kNN, and how missing values are handled. Both deterministic and probabilistic location estimations are confronted with the results of active scanning. For comparability, we perform both types of online scans using identical parameters.

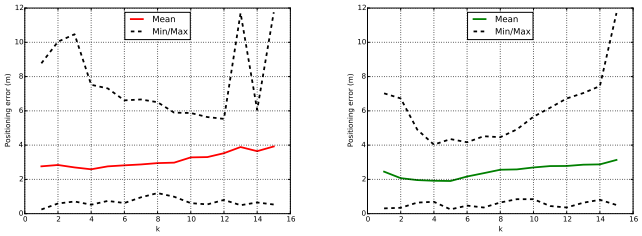
A. Implementation and Setup

We use common active scans for recording the radio map, as this step is not sensitive to users' privacy. The active scans are performed by an application on a Samsung Galaxy S2 (I9100) which is used as our test device. At each reference point, we perform 20 active Wi-Fi scans for each of the four main directions. A series of scans is always annotated with the position of the corresponding reference point on the map and the user's orientation when the fingerprint was taken. For radio map generation in the deterministic approach, each entry in the



(a) Reference points for the radio map marked as blue dots. (b) Locations of position fixes marked as red dots.

Fig. 1. Schematic overview of our test setup.



(a) Active scanning. (b) Passive scanning.

Fig. 2. Comparison of active versus passive Wi-Fi fingerprinting considering missing values, weighted kNN, and user orientation.

fingerprint database represents the vector of the means of 20 consecutively measured RSSI values per reachable AP. For the probabilistic approach, we determine the fingerprint as normal distribution over the measurements of each AP and add the corresponding room label information. Totally, we recorded 332 fingerprints on 83 reference points located within one aisle of our building and its main corridor, as shown in Figure 1a. The distance between consecutive reference points is ever lower than 1.5 meters.

For a fully privacy preserving approach, any active bidirectional communication with a central location server has to be avoided. Instead, the radio map can either be locally stored on the user's device or might be transmitted piece by piece in the beacon frames' optional information element section, as successfully shown in [3]. For our evaluation, however, we skip this step and store the radio map directly on our mobile test device.

In order to make management frames usable for passive fingerprinting, the device's Wi-Fi card has to be set into monitor mode, which is not possible with all common phones. Hence, we first rooted the phone installed a patch for the Wi-Fi card using the Android application package of Bcmon[1], in order to be able to use 802.11 monitor mode for recording beacons. Notice, that when the Wi-Fi card is set into monitor mode, the device is only listening and does not send out any packages that could be captured by a malicious party or infrastructure provider. This can hence be seen as the highest possible level of protecting a users from Wi-Fi based location tracking, while still being able to offer Wi-Fi based indoor positioning and navigation.

In order to create passive fingerprints during the online phase, the mobile device listens on incoming beacon frames for a specific time interval Δt, switching between the most commonly used Wi-Fi channels 1, 6, and 11 after Δt_h. If not explicitly stated otherwise, we set Δt to 3 seconds, and Δt_h to 1 second in our experiments. All necessary information, such as hardware addresses of access points, and corresponding RSSIs, is then extracted from the resulting dump file and a fingerprint is constructed containing the mean values $\overline{v_i}$ of the observed RSSI values for each seen access point i.

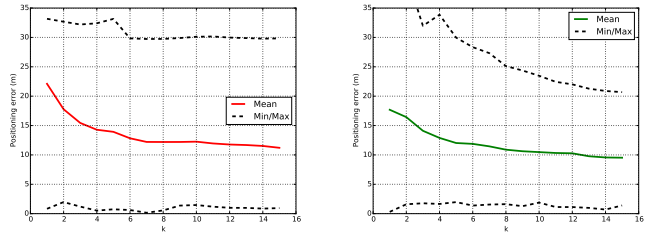
Active fingerprints are created by using the same application as for generating the radio map. One active scan required about 4.5 seconds on average. Thus, our passive approach with $\Delta t = 3$ needs less time to collect the data necessary for formulating a position fix query. To allow for direct comparisons of the active and passive fingerprinting approaches, we successively apply both methods during the online phase on the same device at 19 randomly chosen locations, as indicated in Figure 1b. For determining the user's orientation, we use a digital compass derived from the smartphone's accelerometer and magnetometer sensor readings. Both the orientation information and the observed fingerprint are compared fed to the locally stored radio map using either deterministic or probabilistic location estimation.

B. Deterministic Location Estimation

For evaluation, we calculate the mean, minimum and maximum positioning error, as well as the standard deviation considering all of the 19 active versus the 19 passive position fixes while iterating over different values of k. Figure 2 indicates the results of this real-world experiment when both the user's orientation and missing RSSI values are considered and a weighted kNN approach is used for deterministic location estimation. The best results are obtained with $k = 4$, showing a mean positioning error of 1.92 meters and a standard deviation of 0.92 meters for passive scans, and 2.59 meters with a standard deviation of 1.68 meters in case of common active scanning. Hence, these results indicate that the passive approach performs more accurately within our test set. Furthermore, and as expected, it can be observed that for both scan types, the mean positioning error tends to increase for higher values of k.

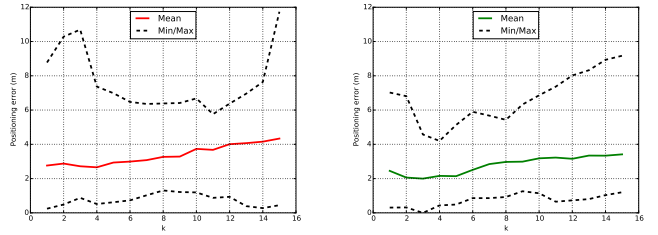
In order to investigate the impact of the used parameters, we now successively compare the results obtained by ignoring missing values, using non-weighted kNN, and completely neglecting the user's orientation. Eventually, the optimal parameter setting that results in the lowest average positioning error will be determined and discussed. Figure 3 indicates the results for active and passive fingerprinting, when missing RSSI values are ignored, but relative weighting and orientation are still considered for location estimation. It is clearly shown, that missing values should be treated by applying a minimal value, as described in Section III-B2. Otherwise, as shown in Figure 3, the obtained values show unfeasible positioning

[1]https://code.google.com/p/bcmon/



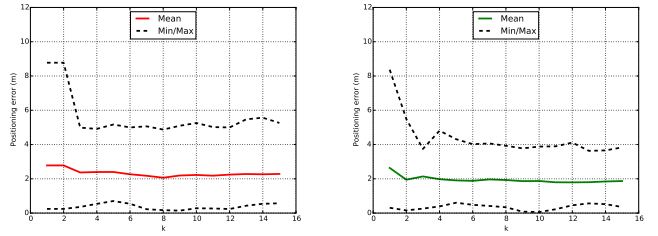
(a) Active, ignoring missing values. (b) Passive, ignoring missing values.

Fig. 3. Comparison of active versus passive Wi-Fi fingerprinting using weighted kNN, and users' orientation, but ignoring missing values.



(a) Active, with non-weighted kNN. (b) Passive, with non-weighted kNN.

Fig. 4. Comparison of active versus passive Wi-Fi fingerprinting using weighted and non-weighted kNN.



(a) Active, without orientation. (b) Passive, without orientation.

Fig. 5. Comparison of active versus passive Wi-Fi fingerprinting when considering and ignoring the users' orientation.

results both for the active and the passive approach. In our case, we observe a mean position error of over ten meters for both scan types and $k < 10$. The standard deviation is greater than 8 meters for active and greater than 6 meters for passive scanning, which is not suitable. These observations are contrary to SMARTPOS, where the authors decided to ignore missing values in order to achieve slightly better positioning results.

As next step, we use a non-weighted kNN while considering the user's orientation and treating missing RSSI values. Again, the obtained results are shown in Figure 4 for both scan types. It can be seen that the mean positioning error is a bit higher for each value of k and for both approaches when using non-weighted kNN instead of weighted kNN. With $k = 4$, the mean accuracy lies at 2.66 meters for active, and at 2.16 meters for passive fingerprinting with a standard deviation of 1.2 meters and 1.7 meters, respectively. Hence, our passive approach returns more accurate position fixes even when a non-weighted kNN location estimator is used. Overall, weighted kNN is to be preferred for both scan types, which conforms to the conclusions made in SMARTPOS.

As a last parameter, we investigate the impact of the user's orientation. Thus, we apply weighted-kNN, consider missing values, but now ignore the orientation information for our location estimation. Figure 5 shows the corresponding results for active and passive fingerprinting. It can be observed that the overall positioning error on average is slightly lower for both scan types, especially for higher values of k, and again passive scanning results in a lower positioning error than the common approach. For active scanning with $k = 4$, the mean accuracy is at 2.40 meters and a standard deviation of 1.52 meters is obtained. This is a tiny improvement of 0.19 meters in terms of accuracy and 0.16 meters in terms of precision for active fingerprinting. In case of our passive approach with $k = 4$, we observe a little degradation of 0.06 meters for both accuracy and precision when ignoring the user's orientation instead of considering it. However, for $k = 6$ a mean positioning error of 1.88 meters and a standard deviation of 0.99 meters is obtained, indicating a slightly improvement of 0.04 meters. An interesting observation is that for higher values of k, the mean accuracy remains constant when ignoring orientation while it is increasing when considering the orientation information. The explanation is, that in case of ignoring orientation, the RSSI vector of online measurements is compared to the complete database, rather than comparing only entries with corresponding orientation. Thus, more similar fingerprints are available for k nearest neighbors, and hence, an increasing k is less likely to negatively influence the positioning result. However, when neglecting orientation information, deterministic location estimation requires 4 times more database comparisons, and thus, a position request takes more time to be served.

In summary, we obtain the best results for both scan types within our experiment when using weighted kNN, considering missing values instead of ignoring them, but ignoring the user's orientation. These findings are contrary to SMARTPOS, where the information of users' orientation helped to increase the positioning accuracy. In our case for passive fingerprinting, the mean positioning error remains constantly below 2 meters, the standard deviation below 1.1 meters for $k > 3$. In comparison, the best results for active scanning were achieved with $k = 8$, showing an accuracy on average of 2.06 meters and a standard deviation of 1.8 meters. Hence, with respect to these results based on deterministic location estimation, we conclude that our passive approach performs slightly better than common active Wi-Fi fingerprinting within our test set.

C. Probabilistic Location Estimation

We apply the naive Bayes classifier as described in Section III-B3 to the same 19 position fixes of our online phase. In order to use the classifier, we first partition our test environment into 19 different rooms and corridor segments. Each

TABLE I
CLASSIFICATION RESULTS FOR ACTIVE AND PASSIVE SCANNING (CORRECT=GREEN, NEARBY=YELLOW, FALSE=RED)

	Active Scanning		Passive Scanning	
Real room	-o	+o	-o	+o
hall	hall	corU3	g001	hall
corL2	corL2	corL2	corL2	corL2
g002	g004	g004	corU1	toilets
corL1	g006	g006	corL1	corL1
corU2	stairs	g004	g001	g003
g002	g002	toilets	g001	g001
g009	g009	g009	g009	g009
g008	g008	toilets	g008	g001
g006	g006	corL2	g006	g006
g003	corL1	corL1	g003	g003
g001	g001	g001	g003	g001
corL2	g010	g010	g009	corL2
corL1	g007	g008	g007	g007
corU2	toilets	toilets	corU2	g007
g010	g006	g006	corL2	corL2
g010	g006	g006	g010	corL2
g010	g010	g010	g010	g010
g004	toilets	g001	g004	corL1
corU3	g001	g001	corU3	g001
Summary				
correct	8	4	11	9
nearby	5	8	5	5
false	6	7	3	5

segment contains four to six reference points marked with the corresponding room label. A room segment is classically divided by its walls, except the segments mapped onto the corridors of the building, which are quite long and are hence further divided into several parts to allow for a fine-grained positioning. Overall, we investigate the correctness of the classification result for each position fix in three categories: correct, nearby (direct neighbor of the actual room) and false. As before, we evaluate the impact of user's orientation by considering (+o) and ignoring (-o) the orientation information for both active and passive scans. The classification results for the complete test set are depicted in Table I.

The best results are obtained for both scan types when the information about users' orientation is ignored, which confirms to SMARTPOS. When orientation is ignored, 42% of all rooms are classified correctly and 31% are false results using common active fingerprint. In comparison, when using our bFP, 58% of all rooms are classified correctly with only 16% being misclassified. Based on these results, we conclude that passive Wi-Fi fingerprinting performs more accurately for both deterministic and probabilistic location estimations, and furthermore, it is capable to completely preserve mobile users' privacy during the whole positioning process.

V. CONCLUSION

In this paper, a privacy preserving Wi-Fi fingerprinting approach was presented and evaluated. The proposed method uses only passive Wi-Fi scans and a locally available radio map. This ensures the highest level of privacy preservation, due to the fact that no signals are sent out by the mobile device. Thus, neither the location provider nor any third party is able to track the device without the user's awareness, which is easily possible using common fingerprinting methods.

Several real-world experiments were conducted using the existing Wi-Fi infrastructure of our office building for the system's evaluation. The obtained results lead to the conclusion that our passive positioning system performs at least as good as common active Wi-Fi fingerprinting approaches in terms of accuracy and precision. One explanation for this observation is that even quick passive scans are able to aggregate more information about received signal strengths for calculating an online fingerprint than common active scanning. This finding is backed by the observation that the precision of our bFP even increases when performing longer scanning periods.

In summary, the best results for both active and passive fingerprinting were obtained using weighted kNN, treating missing RSSI values, and ignoring the user's orientation. With these findings being contrary to some related investigations, further experiments on bigger datasets at other environments have to be conducted for future work in order to verify our findings. Furthermore, we plan to extend our investigations on other commonly used probabilistic location estimations, e.g., Kalman or particle filters. Finally, we want to further discuss and prove the practicality of our proposed privacy preserving positioning approach.

REFERENCES

[1] P. Bahl and V. N. Padmanabhan, "Radar: An in-building rf-based user location and tracking system," in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2. Ieee, 2000, pp. 775–784.

[2] C. Koweerawong, K. Wipusitwarakun, and K. Kaemarungsi, "Indoor localization improvement via adaptive rss fingerprinting database," in *Information Networking (ICOIN), 2013 International Conference on*. IEEE, 2013, pp. 412–416.

[3] F. Gschwandtner and C. K. Schindhelm, "Spontaneous privacy-friendly indoor positioning using enhanced wlan beacons," in *Indoor Positioning and Indoor Navigation (IPIN), 2011 International Conference on*. IEEE, 2011, pp. 1–8.

[4] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in wifi fingerprint-based localization," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 2337–2345.

[5] L. Schauer, M. Werner, and P. Marcus, "Estimating crowd densities and pedestrian flows using wi-fi and bluetooth," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014.

[6] V. Honkavirta, T. Perälä, S. Ali-Löytty, and R. Piché, "A comparative survey of wlan location fingerprinting methods," in *Positioning, Navigation and Communication, 2009. WPNC 2009. 6th Workshop on*. IEEE, 2009, pp. 243–251.

[7] M. Kessel and M. Werner, "Smartpos: Accurate and precise indoor positioning on mobile phones," in *Proceedings of the 1st International Conference on Mobile Services, Resources, and Users, Barcelona*, 2011.

[8] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in *Proceedings of the 5th international conference on Mobile systems, applications and services*. ACM, 2007, pp. 246–257.

[9] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-preserving indoor localization on smartphones," 2015.

[10] *IEEE Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Computer Society, 3 Park Avenue, NY 10016-5997, USA, June 2007.

[11] A. Musa and J. Eriksson, "Tracking unmodified smartphones using wi-fi monitors," in *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*. ACM, 2012, pp. 281–294.

[12] T. King, S. Kopf, T. Haenselmann, C. Lubberger, and W. Effelsberg, "Compass: A probabilistic indoor positioning system based on 802.11 and digital compasses," in *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*. ACM, 2006, pp. 34–40.