# INDOOR SMARTPHONE NAVIGATION USING A COMBINATION OF WI-FI AND INERTIAL NAVIGATION WITH INTELLIGENT CHECKPOINTS

H. Hofer, G. Retscher \*

Dept. of Geodesy and Geoinformation, TU Wien – Vienna University of Technology, Gusshausstrasse 27-29, 1040 Vienna, Austria guenther.retscher@tuwien.ac.at – h.hannes@gmx.at

**KEY WORDS:** Wi-Fi positioning, location fingerprinting, waypoint navigation, intelligent checkpoints, inertial navigation, smartphone inertial sensors, accelerometer, gyroscope, magnetometer, sensor fusion

# ABSTRACT:

For Wi-Fi positioning location fingerprinting is one of the most commonly employed localization technique. To achieve an acceptable level of positioning accuracy on the few meter level, i.e., to provide at least room resolution in buildings, such an approach is very labour consuming as it requires a high density of reference points. Thus, the novel approach developed aims at a significant reduction of workload for the training phase. The basic idea is to intelligently choose waypoints along possible users' trajectories in the indoor environment. These waypoints are termed intelligent checkpoints (iCPs) and serve as reference points for the fingerprinting localization approach. They are selected along the trajectories in such a way that they define a logical sequence with their ascending order. Thereby, the iCPs are located, for instance, at doors at entrances to buildings, rooms, along corridors, etc., or in low density along the trajectory to provide a suitable absolute user localization. Continuous positioning between these iCPs is obtained with the help of the smartphones' inertial sensors. While walking along a selected trajectory to the destination a dynamic recognition of the iCPs is performed and the drift of the inertial sensors is reduced as the iCP recognition serves as absolute position update. Conducted experiments in a multi-storey office building have shown that positioning accuracy of around 2.0 m are achievable which goes along with a reduction of workload by three quarter using this novel approach. The iCP concept and performance are presented and demonstrated in this paper.

# 1. INTRODUCTION

Precise navigation in indoor environments is still a great challenge. The use of wireless technologies for data communication, such Wireless Fidelity (Wi-Fi), for localization has become very popular due to already available infrastructures in many indoor environments. Furthermore, the localization capability of this absolute positioning technology is increasingly augmented with inertial navigation (IN) (Harle, 2013) as smartphones have nowadays built-in motion (i.e., inertial) sensors, such as accelerometers and gyroscopes as well as magnetometers, apart from wireless technologies. The aim of this study at hand is to combine the measurement data of these components and to improve thereby the positioning accuracy and performance of user localization and tracking while reducing the workload required for Wi-Fi positioning. Thus, an approach is developed which uses certain waypoints and makes use of position changes obtained from IN between these points for continuous navigation. These waypoints - termed intelligent checkpoints (iCPs) in the paper - should be recognized by means of Wi-Fi fingerprinting and the relative position changes between them with the help of the inertial sensors. Special attention has to be paid to the entrances of a building, so that the switch between GNSS which is usually employed outdoors and indoor navigation can be achieved.

The paper is organized as follows: In section 2, the concept of the recognition of waypoints using the Wi-Fi module is introduced. Then the field test area and data recording and analyzing system are presented in section 3. Results for Wi-Fi fingerprinting on the selected intelligent waypoints (iCPs) are described in section 4. Section 5 shows how the passing time of an entrance or waypoint was determined during the tests. Section 6 explains how the recognition of waypoints can be used to correct an IN calculated position. In this section, the positioning results achieved with the iCP approach are also presented. Finally, a summary and outlook are given in sections 7 and 8 respectively.

# 2. OPERATIONAL PRINCIPLE OF THE INTELLIGENT CHECKPOINT (ICP) CONCEPT

For the navigation in buildings it is required to determine the current user's location with a positioning accuracy better than a few meters to be able to guarantee at least room resolution. To reach a desired location, it is obvious that certain waypoints need to be passed along the chosen way. First, the building has to be entered via an entrance. After an entrance was chosen, in many cases one will reach a hallway or similar area. To reach other floors, either the elevator or the staircase has to be used. Before reaching one's destination, a person has to walk along a corridor from the previous waypoint to the next. At the destination, usually a door has to be selected to enter the desired room. These waypoints depend on each other and have to be passed following a logical sequence to reach the destination. Doors, staircases and elevators, crossings of corridors, etc., can serve as waypoints or nodes defining vectors of a graph of the path to be used. Moreover, a building can be considered as layers of an onion. Many layers have to be removed to finally reach the inner core. Applied to buildings, the entrances are located in the first layer, the halls in the next layer, corridors and staircase which can be reached by the

<sup>\*</sup> Corresponding author

entrances directly are then to be found on the second layer. The inner core represents the doors to the rooms of the buildings, so they are on the final layer. Figure 1 illustrates these two representations and relationships.

If it is possible to recognize the chosen waypoints and if the relationship between these points is known, the trajectory can be reconstructed. In order to be able to calculate a user's chosen path in real time, it is not enough to simply update the current position once a waypoint is passed. For a continuous positioning calculation, the changes of the positions between these points have to be recognized as well. An obvious solution for tracing position changes are IN systems. Another aim is to recognize which waypoint is passed at what time. The better the recognition of these waypoints, the higher the position determination accuracy. High positioning accuracy is very important for indoor navigation. Finally, it should be possible to show a user his trajectory to a single small room. For the detection of these waypoints, individual pattern characteristics are needed, which can be recorded easily. With smartphones, different sensor data can be obtained, that can then be used for indoor navigation. A common indoor positioning strategy uses the pattern of the received signal strengths (RSS) of available Wi-Fi access points (APs) to calculate the current position of a Wi-Fi receiver. The strategies are able to achieve an accuracy under 10 m (Jekabsons, 2011; Zandbergen, 2009). For Wi-Fi fingerprinting which was introduced in Bahl and Padmanabhan (2000) a raster of positions is defined, where reference RSS values for each position are recorded in a trainings phase. Using a best match scenario, the current RSS values of a Wi-Fi scan are used to find the best match of RSS values in a database in the positioning phase and thus the best matching position. Wi-Fi fingerprinting is explained in more detail in the third section.

It makes sense to use the pattern of RSS values to recognize chosen waypoints, especially if one looks at the further characteristics of Wi-Fi signals. Let us imagine an idealized

model of an AP in which the radiation power is the same in all orientations. If the signal is not attenuated by external influences, it becomes more and more weaker with the distance to the AP. If these RSS values are plotted in a radio map, they would look similar to the pattern of signal strengths from the RFID (radio-frequency identification) tag as illustrated in Figure 2. If more AP are used in a Wi-Fi network, a more complex radio map would be created as a result. Regarding fingerprinting, these AP are treated independently, not as shown in Figure 2 where the strongest signal of an AP of the network is shown. Figure 2 shows the coverage of an observed Wi-Fi network in the test area with multiple APs (Retscher, 2007). The signal strength can also decrease when obstructions are existing in line-of-sight (LOS) from the AP to the receiver caused by materials such as glass, concrete or plasterboard. This means that the RSS to certain APs can change significantly by making small changes in position, when an obstruction reduces the signal strength. This is the case especially at doors, corners and bottlenecks such as entrances to corridors. This fact strongly influences the recognition of the waypoints: If there is an individual RSS distribution for a certain waypoint, it is easier to distinguish this point from other waypoints. This pattern changes as displayed in Figure 2, according to zones of interest for the waypoints such as at the end of the staircases, entrances to corridors and office doors. We call these distinctive waypoints intelligent checkpoints (iCPs) (Retscher and Hofer, 2015). In the case of Wi-Fi fingerprinting, scans of the RSS have to be performed on these iCPs, which will be discussed more in detail in section 4. The iCPs are intelligent in two ways, i.e., because they depend on their intelligent selection for the Wi-Fi RSS scans and because of the logical sequence in their correct order along the trajectory. Further information from smartphone sensors can be used in addition to make the iCPs even smarter. For example, also the passing orientation for some iCPs for the recognition can be used because usually doors have to be passed with a certain orientation. This will be explained in section 5.



Figure 1. Layers and model of a possible trajectory



some e.g. for zones of interest

Figure 2. RSS distribution of observed APs and zones of interest for iCPs (after Retscher, 2007)



Figure 3. Field test site in a multi-storey office building



Figure 4. Overview of the main components of the DAAS

### 3. TEST AREA AND DATA RECORDING

The results which are presented in this paper are based on RSS observation data recorded in front of and inside a multi-storey office building of the Vienna University of Technology (TU Wien). The tests were performed at the entrance area of staircase 1 (see Figure 3(a)) and along the corridor and rooms on the third floor of the building (see Figure 3(b)). On the ground floor, at the four entrances to the building, the location of four iCPs (highlighted in blue in Figure 3(a)) were chosen in a way that it is possible to investigate where they should be located ideally. The location of iCP 1 and iCP 2 is between the

two doors of the porch entrances. The iCP 12 is located outside the building in front of the emergency exit of staircase 1. Apart from the main entrance there is also a side entrance where the iCP 111 is located behind the door on top of the four stairs leading to the ground floor. These four entrance iCPs belong to the entrance layer 0 (see Figure 1). For the tests, on the third floor of the building iCPs 335, 333 and 331 are located around two steps behind the doors to the offices. The iCP 334 is located in a classroom of the institute. They are highlighted using green circles in Figure 3(b) and belong to layer 3. In the layers in-between, another 15 iCPs were defined. Two calibration runs on different days were carried out with a total of 23 candidates for iCPs. In every run, for each of the four orientations five Wi-Fi scans were recorded with a newly developed Android App. Thus, there are 696 scans available in total for the analyses. Additional eight test runs were carried out for the fingerprinting positioning phase.

For the data acquisition and evaluation, a data recording and analysing system (DAAS) was developed which consists of an Android Application (called Combined Positioning System App, CPS) and a framework of MATLAB functions. An overview of the main components of the App and framework of the DAAS is shown in Figure 4, where the integration of the used smartphones is also illustrated. The test devices included the following smartphones: Samsung Galaxy S2 (GT-I9100) with Android 4.1.2 (API 16) and HTC EVO 3D (X515m) with Android 4.0.3 (API 15).

The CPS App can record RSS values and orientation data on selected locations with the 'CPS Kompass WiFi-Scanner' tool. With this tool, the data of Wi-Fi scans can be linked with meta data such as position ID, orientation ID and a comment regarding the scan. The Wi-Fi scans can be defined as calibration data to generate a fingerprinting database in default configuration. If the checkbox 'testscan' is activated, the data can be used as test data for the simulation of positioning. The 'CPS Kompass WiFi-Scanner' is used to record Wi-Fi scans on static positions. Along a trajectory, the tool 'CPS Sensor-WiFi-Recorder' can be used to continuously record RSS values and sensor data. This tool allows the user to define a reference trajectory using rectilinearly connected reference positions. While a person is walking along the trajectory, the arrival time at the defined reference points can be confirmed manually by pressing a button with the App. In that way the reference path for the recorded data on the trajectory can be created. Besides the Wi-Fi scans, the 'CPS Sensor-WiFi-Recorder' records the observations from the accelerometer, barometer, orientation sensor and GPS receiver and stores them, together with timestamps, in the CPS data directory. This directory can be synchronized with a dropbox directory using the Apps 'dropBox' and 'dropBox Sync' which makes it easy to collect data with several devices.

The evaluation kit using the MATLAB framework facilitates various analyses. The framework uses four main datatypes and the MATLAB structure '*wifiscans*' includes all Wi-Fi scans and meta data which are measured in the training (or calibration) phase. On the other hand, the structure '*testscans*' contains the Wi-Fi scans for the positioning phase. The structure '*testscans*' includes the Wi-Fi scans, sensor and GPS data and information to reference positions of the recorded trajectories. Finally, the structure '*Maps*' includes maps of the test areas and GPS mapping information.

#### 4. WI-FI FINGERPRINTING ON ENTRANCES AND OFFICE ICPS

In contrast with Time-of-Arrival (TOA) approaches, Wi-Fi fingerprinting uses received signal strength (RSS) observations directly. Other RSS approaches, such as (tri)lateration, estimate the distance to the corresponding APs from the RSS measurements indirectly. When it comes to fingerprinting techniques, reference positions are defined and Wi-Fi scans are carried out on these points. In a single Wi-Fi scan, the RSS of all available APs are measured. That means that for the reference positions, a database of reference Wi-Fi scans has to be established in a calibration phase. Depending on room size,

two to five reference points were measured in the investigated indoor test site in previous work (Retscher, 2012). For positioning, the Nearest Neighbor (NN) fingerprinting algorithm first presented in Bahl and Padmanabhan (2000) was used. This algorithm calculates vector distance values between a Wi-Fi scan for positioning and all reference Wi-Fi scans in the fingerprinting database. These values describe a quantitative similarity between the position scan and the scans in the database. Thus, the minimal distance value has the best similarity. Most commonly, the Euclidean distance is used for this purpose. The use of other vector distances has been investigated by Moghtadaiee and Dempster (2015) and Retscher and Joksch (2016). No significant differences were seen in their results. Thus, only the Euclidean distance is used in this research. Equation (1) describes the calculation of the distance value  $d_i$  from the Wi-Fi scan for positioning with the RSS values SposAPj for available j access points APj to the measured reference RSS values Sref\_iAPj at the reference position with ID *i* in the fingerprinting database.

$$d_{i} = \sqrt{\left(\sum Spos_{APj} - Sref_{-i_{APj}}\right)^{2}}$$
(1)

With the NN algorithm, a current position can only be assigned to the reference position with the minimum value  $d_i$ . Positions between these reference points cannot be calculated. The K-Nearest-Neighbor (KNN) (Jun et al., 2008) uses k reference positions to calculate a current position between them. For the investigation of the iCP approach, however, our intention was to recognize single reference points. Thus, the NN algorithm is useful for this approach.

In Retscher and Hofer (2015) Wi-Fi fingerprinting was carried out in a logical sequence for the test area. In this approach, the fingerprinting algorithm is applied for each layer separately, which means that for each database query only the reference points in the same layer are considered. In previous work, different variants of averaging strategies for the RSS values in the fingerprinting database were investigated. Furthermore, calculation variants without averaging were investigated, where all Wi-Fi scans from the training phase were used. With this method, a position can be represented by any number of measured Wi-Fi scans. It is also possible to consider the best k matching Wi-Fi scans and choose the reference point which occurs most in the k best scans. With this strategy, better results for the recognition were achieved for iCPs in close proximity. Regarding fingerprinting, usually a position is measured in four different phone orientations. So if more reference Wi-Fi scans are used for the fingerprinting, each orientation has several references in the database. The number of references to be considered can be reduced by a factor of four, without losing accuracy, if the orientation information is used to filter the reference scans with the same orientation (Retscher and Hofer, 2016). By applying this separate fingerprinting strategy for each layer, an average recognition rate of 92.9% for all layers was achieved. Conventional fingerprinting for all investigated iCPs only achieved a rate of 76.9%.

Figure 5(a) shows detailed results for the entrance iCPs with different tested NN fingerprint strategies. The blue bars show the recognition rate for each iCP using the common fingerprinting strategy. In this case, every reference in the database was considered. The references were generated by averaging RSS values and using a minimal value for

inaccessible AP. In the test site, so-called multiple SSID networks exist providing four different Wi-Fi networks at the same physical AP location. The orange bars represent the fingerprinting results in the multiple SSID networks where only one representative network was used. The yellow bars show the results with sequential fingerprinting and multiple SSID considered. With the sequential fingerprinting approach, only the iCPs in the same layer are considered and the best fingerprinting strategy is used. Finally, the green bars show results using weighted RSS values. With this strategy, RSS values from specific APs are weighted higher or smaller for the distance value calculation. To provide a good weighting, an optimization strategy was used. In that strategy a large number of different weighting factors were tested in the positioning phase. The factors with the best recognition rate were stored and used for the further fingerprinting (Retscher and Hofer, 2015). In Table 1 the results for the recognition rates can be seen in more detail. The Table shows that only iCP 2 was incorrectly recognized as iCP 1 two times. In Figure 5(b) the results for layer 3 can be seen. The position of these iCPs are closer to each other than the other iCPs, and in LOS thin walls can decrease the signal. Thus, it is more difficult to distinguish these iCPs. In this layer, the sequential fingerprinting approach is applied using the orientation information of the Wi-Fi scans to achieve a better recognition rate. If a weighted approach of the observations is additionally applied, the recognition rate can be improved from 33% (24/73) to 93% (68/73) for the iCPs in the office layer. Table 2 shows the details of the best results.





(b) Recognition rate for office door iCPs (layer 3)

Figure 5. Recognition rates for entrance iCPs (a) and for office iCPs (b) with several fingerprinting strategies

iCP	recog. rate	Wi-Fi scan references correct and in total	matched points		
1	100.0%	[42/42]	[42x1]		
2	93.3%	[28/30]	[2x1;28x2]		
111	100.0%	[25/25]	[25x11]		
12	100.0%	[29/29]	[29x12]		

 
 Table 1. Detailed results of the fingerprinting strategies for entrance iCPs with the highest recognition rate

iCP	recog. rate	Wi-Fi scan references correct and in total	matched points			
331	100.0%	[27/27]	[27x331]			
333	85.7%	[6/7]	[6x333;1x335]			
334	100.0%	[24/24]	[24x334]			
335	73.3%	[11/15]	[4x333;11x335]			

Table 2. Detailed results of the fingerprinting strategies for office doors iCPs with the highest recognition rate

#### 5. DETERMINATION OF PASSING TIME OF AN ICP

To use an iCP to correct and update an IN position, the passing time has to be determined as precisely as possible. Therefore we analyzed the Wi-Fi scans of the recorded data of the trajectories. In the beginning, we assumed that the passed iCPs are known and only the passing time or step time have to be recognized. That means we have a similar but inverted situation compared with conventional Wi-Fi fingerprinting positioning. Here, a passed position is known, but the time when one had this position has to be recognized based on recorded Wi-Fi scans. Equation 2 describes the calculation of the Euclidean distance  $diCPx_{stepN}$  for all the RSS values  $Sstep_{APj}$  for each step N for available APs j to the reference RSS values  $SiCPx_{APj}$  from iCP x.

$$diCPx_{stepN} = \sqrt{\sum \left(SiCPx_{APj} - Sstep_{APj}\right)^2}$$
(2)

In Figure 6 distance values from the reference RSS values from entrance iCP 2 to the Wi-Fi scans of the data of the TL-EI5 trajectory can be seen in the upper graph in green. For each step or position change, the Wi-Fi scan at that time was taken for the calculation. With the CPS App, the time of passing the iCP 2 was manually recorded in addition. This reference time is shown in the Figure as a red vertical line. The reference step and the calculated step are almost identical; they only have a deviation of one step. The blue line shows the smoothed minimum distance values for the trajectory. For this smoothing calculation, the MATLAB function *smooth*() was used. So in this trajectory the passing of iCP 2 can be recognized up to one step. On average, the passing of an iCP could be recognized with a deviation of 4.9 steps. This deviation could be improved up to 3.6 steps by using the smoothed distance values.



Figure 6. RSS distance values to iCP2 in trajectory TL-EI5

#### 6. TRAJECTORY UPDATE OF INS DEVIATIONS WITH ABSOLUTE POSITIONS

IN suffers from high drifts which accumulate quickly. The iCP algorithm can solve that problem if the passing of a waypoint or an iCP can be recognized correctly. For the presented algorithm, iCPs are used to calibrate positions calculated by IN to the known absolute coordinates of the iCPs. For the plot in the map the algorithm distributes the calculated deviation to the iCP to all steps since the last iCP was passed. This resulted in an improved matching of the reference trajectory. In addition to the Wi-Fi data and the logical possible sequence, the algorithm also uses the current suspected position and orientation of movement to improve the recognition of iCPs. In the defined spheres of influence of iCPs, Wi-Fi scans and the minimal Euclidian distance of RSS values were used to calibrate the position of the IN. For office iCPs, restrictions were defined to make sure that iCPs could only be passed in a certain range of orientation. This is to prevent them from being misrecognized, in case they are passed while a trajectory is located along the corridor. The implemented iCP algorithm uses specific information about the structure of a building at the iCPs. For example, so to calibrate the obtained values of the orientation sensor or change the step size of IN to the stair step length. Figure 7 shows a complete navigation simulation with a smartphone from an outdoor start position to an indoor destination room for two trajectories TL-EI4 and TL-EI8. Here, we assumed that the test area was on the first floor. TL-E4 starts outside across the street at reference point 801 and ends after the first staircase section at reference point 805. The linked trajectory TL-E8 shown in the lower map runs along the stairs and the corridor to room 334. GPS information was only available outdoors. These positions can be seen as blue dots in Figure 7. The iCP algorithm recognizes the correct entrance iCP with a deviation of 3 steps, thus the start position can be calculated with a deviation of 1.5 m only. The estimated step positions of the iCP algorithm are displayed with violet dots on the maps. For the transition between the two trajectories, the result of the end position from TL-EI4 is used as start position for TL-EI8. The iCP algorithm only allowed the passing of iCPs along a logical passing sequence, as introduced in the sequential Wi-Fi fingerprinting section. For each layer, the fingerprinting strategy with the best results (Retscher and

Hofer, 2015) was used by the algorithm. To improve the accuracy, the iCP algorithm uses the known orientations of iCPs to correct the obtained orientation values from an Android system. Additionally, the iCP algorithm changes the step size after passing a staircase iCP to its stair length.



Figure 7. Complete simulation of navigation with a smartphone for two test runs TL-EI4 and TL-EI8

For the trajectories TL-EI4 and TL-EI8, the iCP algorithm achieves an average accuracy of 1.4 m. In comparison to this,

the IN (see purple dots) achieves a deviation of 4.9 m in average, with the reset to the correct start position in all test runs TL-EI. At the entrance, the deviation of the orientation values can be seen in the results of the IN. The problem of stair step size can be seen from the dots of the IN, too. The detailed results for the simulated trajectories are given in Table 3.

#### 7. SUMMARY

The iCP algorithm, which is discussed in this paper, enables seamless transition between GNSS and inertial sensor data supported navigation. This algorithm uses a strategy based on Wi-Fi fingerprinting to recognize the entering of a building. Wi-Fi scans and logical sequences of waypoints (so-called iCPs) are used to recognize their passing. Thus, it is possible to switch between GNSS and indoor navigation at building entrances. In a calibration phase the received signal strength of Wi-Fi APs at the positions of the iCPs are recorded. Then the iCP algorithm uses these RSS values to identify the passing of iCPs. The developed data recording and analyzing system DAAS allows for the recording of the smartphone sensor data along a trajectory by using an Android App. The evaluation is performed with developed MATLAB routines.

In outdoor environment, the algorithm uses GPS positions to add the nearest entrance iCPs to an observing list. If the passing of an entrance is recognized by using reference Wi-Fi scans for the iCPs, the algorithm can switch to inertial navigation. With IN, changes in position can be calculated by using the obtained data from an accelerometer and Android orientation sensor. The orientation sensor is a virtual sensor from the Android system which uses accelerometer and magnetic field sensor data for orientation calculation. With this sensor, the azimuth of the phone can be obtained. The developed algorithm assigns the azimuth value to a detected step at that time and calculates a position change with a definite step length. This representative step length was obtained in calibration measurements for a certain user. While the passing of iCPs is recognized, their absolute position is used to correct the deviation of a current calculated position. The iCP algorithm uses additional information about iCPs and the building structures at their positions to improve positioning accuracy. For example, the step size of the IN is changed if a staircase iCP is recognized; or

the value of the orientation sensor is corrected if an iCP with a specified movement orientation is passed. Data of the orientation sensor was used to improve the identification of the passed iCPs, thus the iCPs to the office rooms have to be passed in a given range of orientation.

For the simulated trajectories the iCP algorithm achieved an accuracy of 1.9 m. In comparison, the inertial navigation with a known start position reached 4.3 m. GPS position, if available, showed an accuracy of only 19.8 m at the recorded trajectories.

# 8. OUTLOOK

The presented algorithm decides which iCP is passed deterministically. If an iCP is passed and it is misrecognized, the iCP algorithm will not work correctly because the following possible logical sequences will be mistaken. A potential solution might be a statistic model, where the passing of an iCP is represented by a probability value. So the possible logical sequence of the iCPs on a trajectory should not be considered as an absolute given deterministic passing order, but it should have influence on the passing probability values. This should prevent the algorithm from complete failure.

Furthermore, the yet static measurement process of iCPs could be developed into a kind of dynamic process. Figure 6 shows the distance values to the static measured reference Wi-Fi scan of iCP 2, which is passed at step 61. The value curve falls abruptly and rises significantly again approximately at steps 55 to 70. That means RSS values before and after the passing of the iCP 2 have a greater difference to its reference Wi-Fi scan. In Figure 8 the RSS values from the available APs in this trajectory data from step 40 to 80 can be seen. The iCP 2 is passed at step 61. Before and after that step, signals of some APs get too weak to be received and signals of other APs start to appear in the Wi-Fi scans. This pattern of passing could be suitable for recognizing the iCP. Instead of a static calibration of the iCPs a dynamic approach could be used. That means multiple Wi-Fi scans are recorded as reference over several steps while passing the iCP. For recognition of the iCPs a calculation based on Euclidian vector distance values between multiple reference Wi-Fi scans and current Wi-Fi scans over several steps could be used.

	average			end position			maximum		
trajectory ID	GPS	IN	iCP algo.	GPS	IN	iCP algo.	GPS	IN	iCP algo.
TL-EI1	34.5	2.9	2.3	36.6	3.5	2.2	45.7	4.3	4.5
TL- EI2	20.7	6.0	4.0	25.8	4.0	2.0	37.4	10.0	11.3
TL- EI3	16.4	3.2	1.9	31.3	3.5	0.0	31.3	6.4	4.8
TL- EI4	12.8	4.3	1.5	22.6	8.5	1.0	22.6	8.5	4.7
TL- EI5	14.7	4.2	1.9	32.2	5.9	1.1	32.2	6.4	5.5
TL-EI6		4.8	1.5		8.7	2.1		9.2	2.7
TL- EI7		3.8	1.1		4.6	3.1		6.9	3.7
TL-EI8		5.5	1.3		6.5	0.5		8.0	3.4
mean	19.8	43	19	29.7	57	15	33.8	75	51

Table 3. Detailed deviations in [m] and comparison for GPS, IN and iCP algorithm



Figure 8. RSS values from the available APs in TL-EI5 from step 40 to 80

# REFERENCES

Bahl, P., Padmanabhan, V. N., 2000. RADAR: An In-building RF-based User Location and Tracking System, INFOCOM 2000, In *19th Annual Joint Conference of the IEEE Computer and Communications Societies*, Tel-Aviv, Vol. 2, pp. 775-784.

Harle, R., 2013. A Survey of Indoor Inertial Positioning Systems for Pedestrians. In *IEEE Communications Surveys and Tutorials*, 15(3), pp. 1281-1293.

Jekabsons, G., Kairish, V., Zuravlyov, V., 2011. An Analysis of Wi-Fi Based Indoor Positioning Accuracy. In *Scientific Journal* of Riga Technical University, Computer Sciences, 44(1), pp. 131-137.

Jun, M., Xuansong, L., Xianping, T., Jian, L., 2008. Cluster Filtered KNN: A WLAN-based Indoor Positioning Scheme. In Ramesh, J., Mohan K. (Eds.): *International Symposium on a World of Wireless, Mobile and Multimedia Networks 2008* (*WoWMoM'08*). Newport Beach, CA, USA, Piscataway, NJ, USA: IEEE Xplore Digital Library, pp. 1-8.

Moghtadaiee, V., Dempster, A. G., 2015. Vector Distance Measure Comparison in Indoor Location Fingerprinting. In *Proceedings of the IGNSS 2015 Conference*, Surfers Paradise, Gold Coast, Australia, 16 pgs. Retscher, G., 2007. Ubiquitous Positioning Solutions for Pedestrian Navigation. In *Proceedings of the 5th Symposium on Mobile Mapping Technology*, Padua, Italy, pp. 250-256.

Retscher, G., 2012. Wi-Fi Positioning with Smartphones. In *Proceedings of the 9th International Symposium on Location-Based Services LBS 2012*, Springer Science, Berlin, Germany.

Retscher, G., Hofer, H., 2015. A Novel Approach for Wi-Fi Fingerprinting Using Logical Sequences of Intelligent Checkpoints. In *Proceedings of the IGNSS 2015 Conference*, Surfers Paradise, Gold Coast, Australia, 16 pgs.

Retscher G., Hofer H., 2016. Wi-Fi Location Fingerprinting Using an Intelligent Checkpoint Sequence. In *Proceedings of the FIG Working Week 2016*, Christchurch, New Zealand, 15 pgs.

Retscher, G., Joksch, J., 2016. Analysis of Nine Vector Distances for Fingerprinting in Multiple SSID Wi-Fi Networks. In *Proceedings of the International Conference on Indoor Positioning and Indoor Navigation IPIN 2016*, Alcalá de Henares, Madrid, Spain, 4 pgs.

Zandbergen, P. A., 2009. Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning. In *Transactions in GIS*, 13(s1), pp. 5-25.