

Gate-Passing Detection Method Based on WiFi Significant Points

Katsuhiko Kaji and Nobuo Kawaguchi

Abstract—We propose a gate-passing detection method based on WiFi signal strength and the accelerometers of user smartphones. Since doors divide such physical areas as rooms and hallways, the WiFi environments tend to greatly vary. A gate should exist when the points in the WiFi environments vary on a large scale. We define such points as WiFi significant points and propose a detection method based on a WiFi distance function and estimated moving distance according to an accelerometer. We evaluated our proposed method and found out that most door passings can be detected. We also found that we can estimate the existence of doors that have identical door passings with a high degree of accuracy.

Index Terms—Door detection, Wireless-LAN, Accelerometer

I. INTRODUCTION

Gate passings, which refer to the entrances and exits to a building or a room and going by a corridor, are crucial information for indoor location-based services, especially for monitoring user activities, recognizing user migration pathways, and lifelogs.

Traditional gate-passing detection methods suffer from the following problems. The most general gate-passing detection method is IC card readers or RF tag readers attached to gates. In such situations, users touch the readers with their cards. The vision-based approach detects a gate [1]. Its door is extracted from the images captured by the camera attached to a robot or a user. The restrictions of camera locations burden general users. Another method uses proximity sensors [2], although general mobile terminals don't have them.

In this paper, we propose a gate-passing detection method. We assume that users have general smartphones. In our method, we use WiFi signal information for gate detection and estimate the moving distance by accelerometers with which most smartphones are equipped. WiFi access points (APs) must be placed in the environment, even though many APs have already been placed in public buildings, universities, and offices.

The following is the outline of our proposed method. Since WiFi signal strength tends to be cut off or reduced by such gates as doors, we assume gates in a location where the WiFi environment greatly varies. To acquire the degree of variation of WiFi environments, we introduce and compare two kinds of moving distances that are based on WiFi and accelerometers. If the WiFi-based distance deviate from the accelerometer-based distance, we assume that the user is passing a gate.

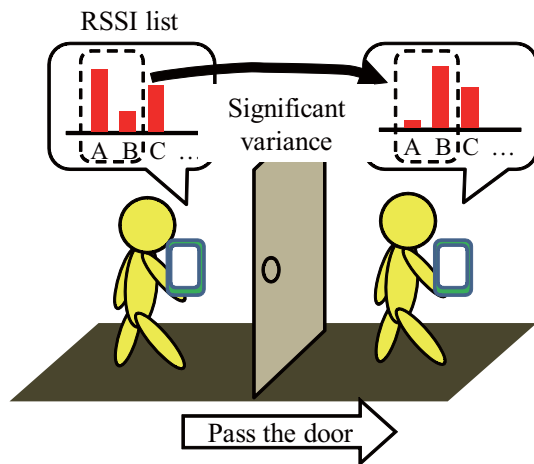


Fig. 1. WiFi environment variation by passing a door

A. Proposed method

Many objects divide spaces, such as doors, elevators, and walls. Such objects tend to cut off or weaken WiFi signal strength. The degree of decay depends on the object's material and the physical relationship between the object and the AP. However, in many cases, WiFi environments separated by objects tend to be very different.

Figure 1 shows an example where a WiFi environment is different because it is separated by a door. If the user passes it, the WiFi environment changes. We assume that if the WiFi environment greatly varies, the user is passing a gate such as a door.

In this paper, we define a location where WiFi environments are separated by significantly different locations as a WiFi significant point. We assume a situation where users have standard smartphones and walk around indoors. Our method requires two kinds of moving distances. One is accelerometer-based step estimation, and the other is the distance based on the variation of WiFi signal strengths and the signal propagation model. If the latter distance deviate from the former distance, the method judges that the user has passed a WiFi significant point.

One typical signal propagation model is the Seidel model [3], which represents the relationship between the distance to an AP and its received signal strength indication (RSSI). With the model, we can estimate the distance to AP using RSSI.

1) *Fundamental algorithm for extracting WiFi significant points*: First, we formulate the WiFi significant point extraction algorithm by defining a simple environment. It has only one AP whose location is unknown. Users walk around it freely, thus the trajectory is not necessarily linear. From WiFi and accelerometer information, two kinds of distances

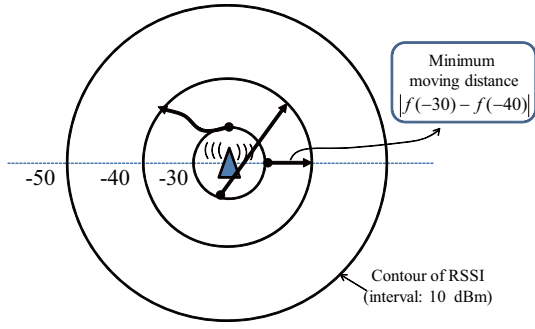


Fig. 2. Possible variation of user trajectory when RSSI varies from -30 to -40 dBm

are estimated.

One distance is user minimum moving distance d_{min} that is estimated by the WiFi information. When RSSI r_{t1} at time t_1 changes to r_{t2} at time t_2 , the minimum moving distance is represented as the following formula using WiFi propagation model f :

$$d_{min} = |f(r_{t1}) - f(r_{t2})|. \quad (1)$$

Figure 2 shows several possible trajectory examples where RSSI is changed from -30 to -40 dBm. When the user linearly moves away from the AP, the lengths of the distance of trajectories must be the shortest. The length is calculated as $|f(-30dBm) - f(-40dBm)|$. If the user passed the WiFi significant point, estimated minimum distance d_{min} should be larger than the actual walking distance.

The other distance, which is maximum moving distance d_{max} between times t_1 and t_2 , is estimated by an accelerometer. Walking steps can be extracted by capturing the periodical local maximum and local minimum values of an accelerometer. Each step's distance is estimated using the user's height and the local maximum and local minimum values. Here, if the user is walking linearly, the distance is the sum of each step's distance. If the user isn't walking linearly, the distance between the user's positions at t_1 and t_2 must be shorter than the distance of the linear walking. The sum of the walking distance must be the maximum distance.

Based on d_{min} and d_{max} , we estimate whether the user passed the WiFi significant point during t_1 and t_2 . The algorithm is shown in Fig. 3. If d_{max} exceeds d_{min} , the actual distance range can be estimated (Fig. 3, top). On the other hand, if the WiFi environment varies significantly during t_1 and t_2 , d_{min} should be larger than the actual walking distance, and d_{min} is probably larger than d_{max} (Fig. 3, bottom). In such situations, we judge that value d_{min} is not reasonable. Consequently, we consider that the user passed the WiFi significant point during t_1 to t_2 .

B. Extending our proposed method for real environments

We introduce the effect of the fluctuation of RSSI and multiple WiFi information and extend our proposed method for real environments. In the real world, WiFi signals influence multipath fading so that RSSI is not constant. Using the average or median RSSI values that are observed multiple times, the effect of fluctuation can be reduced. We imagine a situation where users aren't standing, so WiFi RSSI cannot

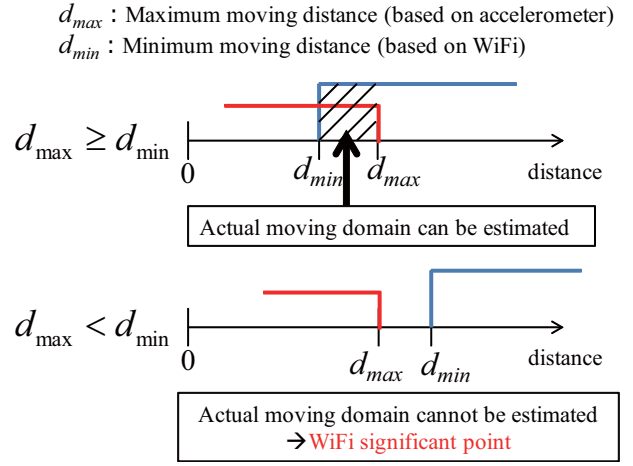


Fig. 3. Fundamental basis of WiFi significant point extraction

be observed multiple times. The effect of fluctuation cannot be ignored. At the same time, we must consider the multiple WiFi information transmitted by multiple APs. Recently, since many APs have been placed in various buildings, we can receive multiple AP signals at a number of locations.

1) *Effect of fluctuation of RSSI*: First, we introduce the effect of the fluctuation of RSSI and reconstruct our above scheme as a stochastic model. In this paper, we approximate the fluctuation as a Gaussian distribution. Several researches adopt Gaussian distribution to approximate RSSI fluctuation [4], [5]. We also regard the level of fluctuation as constant. In ideal environments, the distance can be calculated using function f and RSSI r_μ , and the distance is expressed as $f(r_\mu)$. The fluctuation is expressed as a Gaussian whose average is r_μ and the standard deviation is r_σ (Fig. 4 top). At the time, in the ideal environment, when RSSI is observed, distance $r_\mu - r_\sigma$ can be calculated as $f(r_\mu) - f(r_\mu - r_\sigma)$. Using the value, we approximate the distance fluctuation to AP as a Gaussian distribution where the average is $w_\mu = f(r_\mu)$ and the standard deviation is $w_\sigma = f(r_\mu) - f(r_\mu - r_\sigma)$ (Fig. 4 bottom).

Minimum distance d_{min} , which we introduced above, is expressed as a subtraction of Gaussian distributions. Consequently, minimum distance d_{min} is expressed as a Gaussian whose average is $d_{min_mu} = w_{\mu1} - w_{\mu2}$, and the standard deviation is $d_{min_sigma} = \sqrt{w_{\sigma1} + w_{\sigma2}}$.

In the previous section, the existence probability of WiFi significant points is expressed as binary. On the other hand, by introducing fluctuation, the likelihood based on two kinds of distances d_{max} and d_{min} are expressed as cumulative probability (5 shaded area). The likelihood is calculated as Eq. 2. Here, $erf(x)$ is an error function.

$$p = \frac{1}{2} \left(1 + erf\left(\frac{d_{ref} - d_\mu}{\sqrt{2d_\sigma^2}}\right) \right) \quad (2)$$

The top of Fig. 5 is an example where cumulative probability p is high. In short, the observed RSSI should probably be fluctuated. On the other hand, if p is under threshold $p_{threshold}$ (Fig. 5, bottom), the observed RSSI is unlikely even where the fluctuation is concerned. We assume that a WiFi significant point is passed between observation times t_1, t_2 .

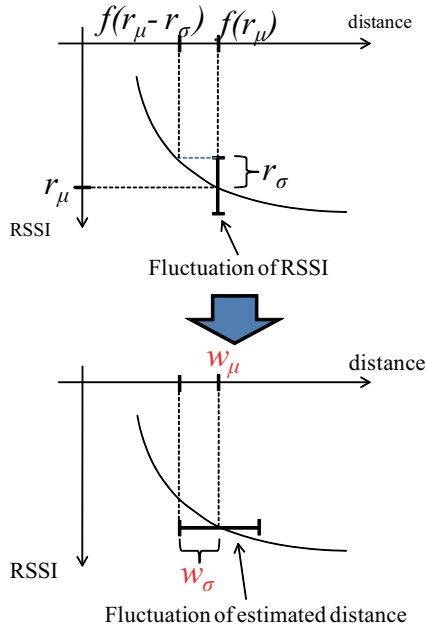


Fig. 4. Conversion from RSSI fluctuation to distance fluctuation. (top: Gaussian distribution of RSSI, bottom: Gaussian distribution of distance)

d_{max} : maximum moving distance (based on accelerometer)
 d_{min_mu} : the mean of minimum moving distance (based on WiFi)
 p : likelihood of the moving distance

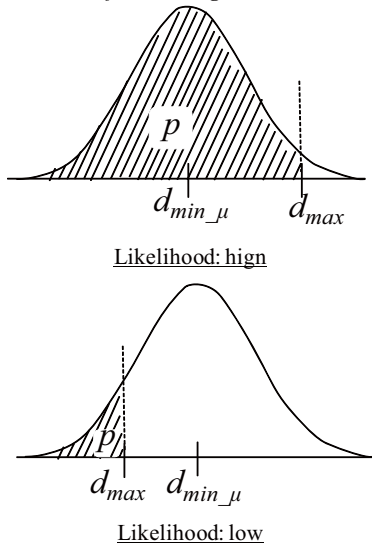


Fig. 5. Distance likelihood

Based on the fluctuation, a weak RSSI value should not be used to extract WiFi significant points. If the RSSI is weak, the estimated distance to the AP is significantly different if the RSSI value is fluctuated. For example, using the WiFi propagation model from the evaluation section, the distance where the RSSI is -80 dBm is 83 m, and the distance where it is -81 dBm is 91 m. The variance is only 1 dBm, but the difference of the estimated distances is 8 m. Therefore, we use RSSI values that exceed threshold $r_{threshold}$ for WiFi significant point extraction.

2) *Multiple APs' WiFi information*: Next, we introduce multiple AP RSSI information. When the user passes a point where the WiFi environment changes significantly, RSSIs

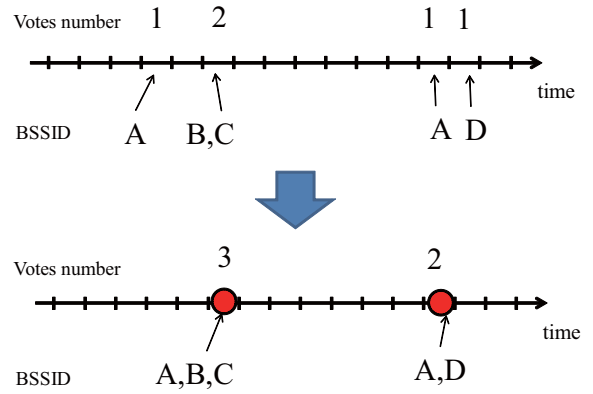


Fig. 6. Voting and aggregation of WiFi significant points. Top: voting, bottom: aggregation

don't always change simultaneously due to the mobile device's sensitivity and the device driver. Thus, the time instants that WiFi significant points are observed don't always match.

To reduce the problem, we aggregate WiFi significant points that come from each AP's RSSI as one WiFi significant point.

Based on the previous section, the existence of WiFi significant points from each RSSI is judged in each observation interval between t and $t + 1$. The WiFi significant points receive votes for their respective intervals. Then the interval that receives the most votes in a window, whose size is w , is deemed to be one WiFi significant point. Fig. 6 shows an example of the voting and the aggregation of WiFi significant points. The window size is 4. In the example, four zones are voted as WiFi significant point at first (Fig. 6 top). Then, according to the voting count and window size, they are aggregated as two zones (Fig. 6 bottom). Finally, these two zones are considered as WiFi significant point.

C. Identical gate-passing detection and passing direction estimation

The aggregated WiFi significant points consist of multiple WiFi significant points from multiple APs' WiFi information. We believe that identical gate-passing detection can be realized using the pattern of the AP's information. The pattern of i -th WiFi significant point S_i is expressed as a vector using the number of votes and voted BSSIDs b .

$$S_i = [b_{i,0}, b_{i,1}, \dots, b_{i,n}] \quad (3)$$

The similarity of two arbitrary WiFi significant points S_i , S_j is calculated using Tanimoto coefficient T [6]:

$$T = \frac{N(S_i \cap S_j)}{N(S_i) + N(S_j) - N(S_i \cap S_j)}. \quad (4)$$

The Tanimoto coefficient is a similarity metric to evaluate two sets. If they are completely identical, T is 1. They don't have a common element, and T is 0. Here, $N(x)$ is the number of elements in x .

When similarity T exceeds similarity threshold $t_{threshold}$, WiFi significant points S_i , S_j are estimated to be the same point, and the user is passing the gate again.

Furthermore, we estimated the passing direction using the pattern of the variance of the RSSIs. For each common BSSID b in S_i and S_j , we checked the variance direction to determine whether RSSI increased or decreased. If the variance direction is the same, N_{same} is incremented. If the variance direction is different, N_{diff} is incremented. If N_{same} is larger than N_{diff} , the user passed the gate from the same direction, and if N_{diff} are larger than N_{same} , the user passed the gate from a different direction.

D. Correction of WiFi significant points using accelerometers

As above, RSSIs don't always change at the gate-passing moment. Based on our pilot study, the difference of the RSSI change timing and actual gate-passing timing is not zero, and the difference may be about ten seconds.

Next we corrected the WiFi significant point with an accelerometer. Generally, when a person passes a gate, the step interval is long, and each step length is short, even though the continuing time of the state is not so long. Based on the heuristics, we developed simple gate-passing timing estimation using an accelerometer. In our method, when the accelerometer's local maximum and minimal are lower than threshold $g_{threshold}$ and the continuing time is lower than $w_{threshold}$, we assume the time zone is a gate passing. Here, $g_{threshold}$ means threshold of gate-acc and $w_{threshold}$ means threshold of gate-passing time.

If the time distance between a WiFi significant point and a gate-passing time is under window size w , the time of the WiFi significant point is corrected to the gate-passing time. When multiple WiFi significant points exist within the window, the nearest WiFi significant point is corrected as the gate-passing time.

Note that our door passing estimation is not very robust. Various situations probably exist where the estimation is not correct. For example, when the environment is crowded, people stand or walk slowly for a short time. The method is probably inaccurate when a person slow down to passes a corridor's corner.

E. Restrictions

Our proposed method is very dependent on the physical relationships between gates and APs. Thus, not all gate passings can be detected by our method. If there are no APs around a gate, gate passings cannot be detected. Even if an AP exists around a gate, there are patterns of physical relationships between the AP and the gate where our method cannot extract gate passings. Fig. 7 shows two of the examples. In such a situation as the top of Fig. 7, the RSSIs at points A and B are almost the same, so the gate passings cannot be extracted by the RSSI variance. In such a situation as the bottom of Fig. 7, the pattern of the RSSI variance of passing rooms C and D is almost the same. Thus, using our proposed identical gate-passing detection, the doors of the two rooms should be detected as the identical door.

Additionally, there are several restrictions to apply our proposed method. First, the gate must physically divide the environment like doors and elevators. Second, the person himself should open a gate to pass. If the door is already open, the RSSI variance cannot be captured.

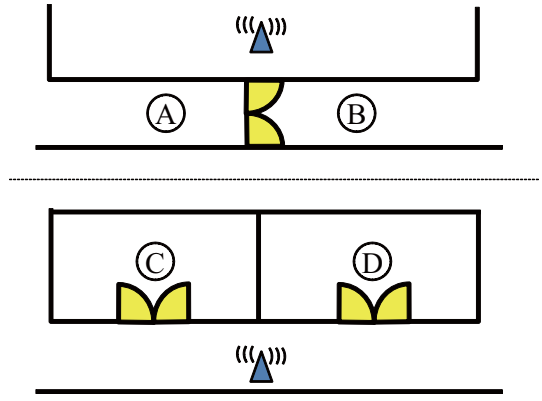


Fig. 7. Examples of situations where it is impossible to apply proposed method

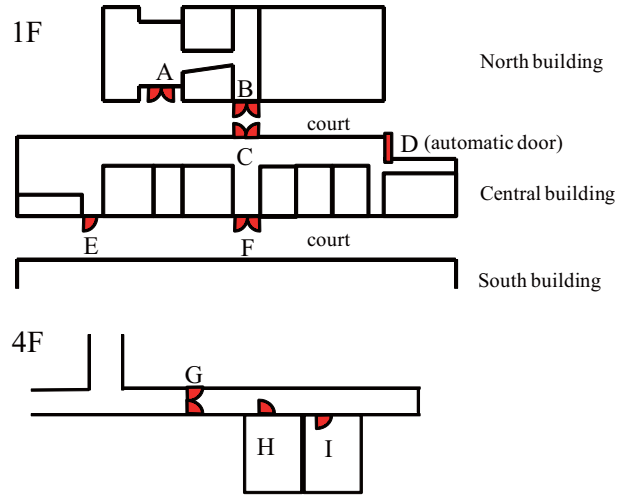


Fig. 8. Door alignment. Top: 1F, bottom: 4F

II. EXPERIMENTS

We experimentally evaluated the accuracy of our method using the gate-passing detection method and the identical gate-passing estimation method.

A. Experimental environment

We conducted our experiment on the 1st and 4th floors of the IB Information Buildings on Nagoya University. The door alignment and types are shown in Figs. 8 and 9. There were nine doors in the environment including one automatic door. Doors A-F are the entrance doors of the buildings, and doors G-I are inside the buildings.

Table I overviews the observation data. The subject is one of the authors of this paper who used an iPhone3G smartphone. He put it in his waist holder and walked around the experimental environment. His walking speed was not constant; standing and slow walking were included except for door passings. Our proposed method is applicable when users themselves open and close doors, so he opened and closed doors when passing them.

B. Settings

We adopted LaMarca's parameter of the Seidel model [7] (Eq. 5).



Fig. 9. Door types

TABLE I
OVERVIEW OF EXPERIMENTAL DATA

Sampling rate of WiFi observation	1 Hz
Sampling rate of accelerometer	100 Hz
Number of doors	9
Number of door passings	A-F: 10 times, BG-I: 20 times
Total experimental time	5300 seconds

$$f(r) = -32 - 25\log_{10}r \quad (5)$$

Step length s is calculated by the following formula [8].

$$s = 0.26 \cdot height + (peakdiff - peakavg) \cdot 5.0. \quad (6)$$

Here, $peakdiff$ is the difference between the value of the local maximum and the local minimum in each step and $peakavg$ means the average value of $peakdiff$. The user's height is $height$. In this experiment, we set the values as $height = 1.80[m]$, $peakavg = 1.11[g]$.

C. Results

1) *Gate-passing detection method*: Table III shows the result of gate-passing detection. We define correct answers to be when a detected gate passing is within 10 seconds of the actual door passing. The precision of the gate-passing detection was about 58%, and the recall was about 76%. Consequently, our proposed method detected about half of the door passings, but it doesn't always detect them.

Figure 10 shows the accuracy of the gate-passing detection for individual doors. The maximum accuracy is 100%, and the minimum accuracy is 40.0%. Based on the results, the accuracy of the gate-passing detection significantly differs by door, even though gate-passing detection is possible when the user passes the door many times.

Automatic doors provide minimum accuracy. When passing automatic doors, the step length around the door isn't shorter than manual doors. This explains why the accuracy

TABLE II
EXPERIMENTAL PARAMETERS

Fluctuation of RSSI r_σ	2.5 dBm
Threshold of RSSI $r_{threshold}$	-60 dBm
Threshold of likelihood $p_{threshold}$	0.1 %
Threshold of similarity $t_{threshold}$	0.4
Window size w	10 sec
Threshold of gate-acc $g_{threshold}$	0.15 G
Threshold of gate-passing time $w_{threshold}$	2.0 sec

TABLE III
ACCURACY OF GATE-PASSING DETECTION

Gate-passing detected points	157
Actual gate passings	120
Successful gate-passing detections	92
Precision	59%
Recall	76%
F-measure	66%

of automatic door passing detection is low. Of course, our method is influenced by the door's material and the distribution of APs. This is one reason that the accuracy of gate-passing detection widely differs by door.

On the other hand, WiFi significant points were detected except for around the gate. One reason is the existence of WiFi hotspots caused by reflections and multipaths. For example, corridor's corner tends to be WiFi hotspot.

2) *Identical gate-passing estimation*: Using successfully detected points (92 points), we evaluated the identical gate-passing estimation. Precision, recall, and F-measure are shown in Table IV. Fig. 11 shows the individual door results of the identical gate estimation. The accuracy of door G is obviously higher than the other doors. Door G is the thickest, and one AP is placed near it. Such an ideal environment enhances the accuracy of identical gate-passing estimation.

The number of errors relevant to doors H and I is 43, 19 of which were mistaken for other doors. Doors H and I are located within 3 m of each other, so the pattern of their WiFi environments is similar.

Consequently, the accuracy of identical gate-passing estimation is not as high as gate-passing detection, even though we found doors on which the identical gate-passing estimation method was successfully performed. Therefore, we believe that our method is useful for restrictive situations.

For 245 pairs that were correctly estimated as the same gate, we applied the gate-passing direction estimation method, and the accuracy was 92%. Additionally, for door G whose accuracy of identical gate-passing estimation was high, the accuracy of the gate-passing direction estimation was 100%. Consequently, the gate-passing direction estimation method is generally useful.

III. RELATED WORKS

There are several researches on gate detection. Patel proposed a person movement detection method based on air pressure sensors attached to HVAC units[9]. The method captures door openings and closings, door-passing based on the variation patterns of air pressure, although a case might exist where air pressure sensors are difficult to attach to HVAC units due to a building's structure. Moreover, if multiple persons exist, this method cannot track an individual.

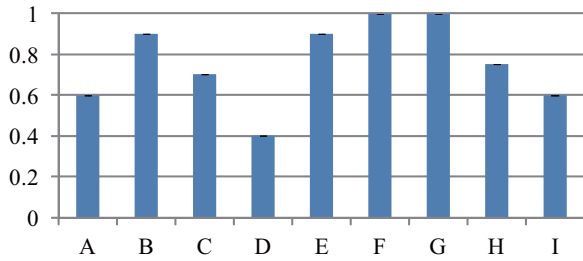


Fig. 10. Gate-passing detection accuracy for individual doors

TABLE IV
ACCURACY OF IDENTICAL GATE-PASSING ESTIMATION

WiFi significant points related to door passings	92
Pair of WiFi significant points that hline have identical gates	348 pairs
Pairs of WiFi significant points where hline identical gate detection was correct	245 pairs
Pairs of WiFi significant points where hline they should be estimated as same gate	508 pairs
Precision	70%
Recall	48%
F-measure	57%

GPS-based building entrance/exit detection methods have also been proposed [10]. Generally, GPS signal strength tends to be weak inside buildings. In our method, with training data that were observed beforehand, we generated a detection model. Therefore, a labor cost problem exists for prior observation. On the other hand, our proposed method needs no preparation.

Hotta proposed a robust room-level location estimation method [11]. When generating WiFi fingerprints, the distance to the nearest door is input. Additionally, they introduced a room transition probability, which is generated using the distance to the nearest door; the probability will be high when the location is near a certain door. Our method doesn't just detect actual door passings; it also enhances the transition probability.

IV. CONCLUSION

We proposed a gate-passing detection method based on WiFi significant points. Our method is based on the assumption that WiFi environments, which are divided by gates, tend to be very different. Only WiFi and accelerometer information are used to detect gate passings. We conducted several experiments and found that our proposed method has the ability to detect more than half of the gate passings. Identical gate-passing detection has very low accuracy. However, we found gates whose accuracy of identical gate-passing methods is high.

One application of our proposed method is the cumulative error correction of dead-reckoning [12]. By using the identical gate-passing detection method, cumulative error can be corrected based on the location passed before and after location.

REFERENCES

[1] Jauregi, E., Lazkano, E., Sierra, B., "Approaches to Door Identification for Robot Navigation," in *Mobile Robots Navigation*, Alejandra Barrera (Ed.), ISBN: 978-953-307-076-6, InTech, 2010, pp. 241–262.

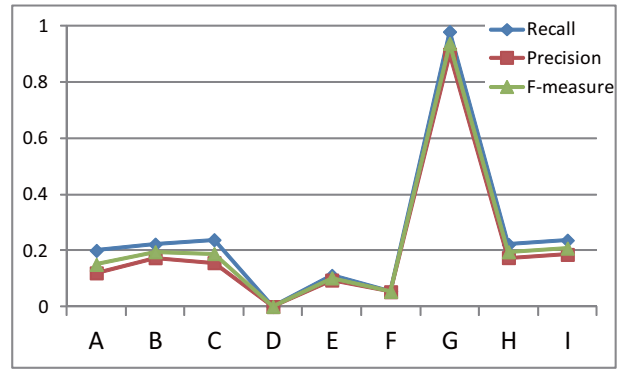


Fig. 11. Accuracy of identical gate-passing detection for each door

- [2] Schindler, G., Metzger, C. Starner, T., "A Wearable Interface for Topological Mapping and Localization in Indoor Environments," in *Proceedings of Location- and Context-Awareness Second International Workshop*, 2006, pp. 64–73.
- [3] Seidel, S., and Pappert T., "914Mhz Path Loss Prediction Model for Indoor Wireless Communications in Multifloored Buildings," in *Proceedings of IEEE Transactions on Antennas and Propagation*, 1992, pp. 207–217.
- [4] Ferris, B., Fox, D., Lawrence N., "WiFi-SLAM Using Gaussian Process Latent Variable Models," in *Proceedings of the 20th international joint conference on Artificial intelligence(IJCAI'07)*, 2007, pp. 2480–2485.
- [5] Goswami, A., Ortiz, L.E., Das, S.R., "WiGEM: a Learning-based Approach for Indoor Localization," in *Proceedings of the Seventh Conference on emerging Networking EXperiments and Technologies(CoNEXT'11)*, 2011.
- [6] Segaran, T., *Programming Collective Intelligence: Building Smart Web 2.0 Applications*. O'Reilly Media, 2008.
- [7] LaMarca, A., Hightower, J., Smith, I., and Consolvo, S., "Self-Mapping in 802.11 Location Systems," in *Proceedings of the Seventh International Conference on Ubiquitous Computing (UbiComp2005)*, 2005, pp. 87–104.
- [8] Anzai, K., Okajima, S., Tsubokawa, H., "The Estimate of the Indoor Position that Used a Smartphone and the Suggestion of the Walk Navigation Systems," in *Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO2011)*, 2011, pp. 921–927.
- [9] Patel, S.N., Reynolds, M.S., Abowd, G.D., "Detecting Human Movement by Differential Air Pressure Sensing," in *Pervasive Proceedings of the 6th International Conference on Pervasive Computing*, 2008, pp. 1–18.
- [10] Katsuda, E., Uchiyama, A., Yamaguchi, H., Higashino, T., "Distinguishing Indoor/Outdoor Using Training Data of GPS Status," in *IPSI SIG Technical Report 2011-MBL-60(18)*, 2011, pp. 1–8.
- [11] Hotta, S., Hada, Y., Yaginuma, Y., "A Robust Room-level Localization Method Based on Transition Probability for Indoor Environments," in *Proceedings of International Conference on Indoor Positioning and Indoor Navigation*, 2012., 2012.
- [12] Kamisaka, D., Muramatsu, S., Iwamoto, T., Yokoyama, H., "Design and Implementation of Pedestrian Dead Reckoning System on a Mobile Phone," *IEICE transactions on information and systems*, vol. 94, no. 6, pp. 1137–1146, 2011.