Indoor Localization Using Multiple Wireless Technologies

A.K.M. Mahtab Hossain, Hien Nguyen Van, Yunye Jin, Wee-Seng Soh

Department of Electrical & Computer Engineering
National University of Singapore, Singapore
Email: {g0500774, u0303567, jin_yunye, elesohws}@nus.edu.sg

***Abstract*— Indoor localization techniques using location fingerprints are gaining popularity because of their cost-effectiveness compared to other infrastructure-based location systems. However, their reported accuracy fall short of their counterparts. In this paper, we investigate many aspects of fingerprint-based location systems in order to enhance their accuracy. First, we derive analytically a robust location fingerprint definition, and then verify it experimentally as well. We also devise a way to facilitate under-trained location systems through simple linear regression technique. This technique reduces the training time and effort, and can be particularly useful when the surrounding or setup of the localization area changes. We further show experimentally that because of the positions of some access points or the environmental factors around them, their signal strength correlates nicely with distance. We argue that it would be more beneficial to give special consideration to these access points for location computation, owing to their ability to distinguish locations distinctly in signal space. The probability of encountering such access points will be even higher when we denote a location's signature using the signals of multiple wireless technologies collectively. We present the results of two well-known localization algorithms (K-Nearest Neighbor and Bayesian Probabilistic Model) when the above factors are exploited, using Bluetooth and Wi-Fi signals. We have observed significant improvement in their accuracy when our ideas are implemented.**

Keywords: Location Fingerprint, SSD, Interpolation, Anchors, Localization, Bluetooth, Wi–Fi, Location Systems.

I. Introduction

Recently, there have been considerable interests in indoor localization techniques. It is generally agreed that a desirable indoor location system should be characterized by high accuracy, short training phase, cost-effectiveness (preferably using off-the-shelf hardware), and robustness in the face of previously unobserved conditions. Our work herein aims to achieve a location system that accomplishes all these requirements.

In future ubiquitous computing environment, location services for handhelds are likely to be in high demand. However, these handhelds are expected to come in with many different hardware solutions, even for the same wireless technology. As a result, a location system that relies solely on *absolute* signal strength measurements to define location fingerprints would not perform well. Regardless of whether a device's signal strengths perceived at the access points (APs) are used to denote the device's location fingerprint, or that the APs' signal strengths perceived at the device are used, such fingerprints may differ significantly with the device's hardware even under the same wireless conditions. This can easily be observed in existing popular wireless technologies, such as Wi-Fi or Bluetooth. The presence of power control in some wireless technologies further complicate the matter.

The need for robust location fingerprint is obligatory for any localization algorithm that utilizes it, no matter how sophisticated the algorithm is. In this paper, we have analytically shown that the *difference* of signal strengths perceived at APs provide a more robust location fingerprint, rather than absolute signal strength values. We also verify our claim with detailed experimental findings. An earlier work [1] only provided experimental results exploiting this idea in order to find a rogue machine, without proper analysis about why signal strength difference should be categorized as *stable* location fingerprint.

Few prior works [2], [3] have attempted to shorten the training phase of a location system. They contend that, rather than performing an exhaustive survey to create a location fingerprint database that requires substantial cost and labor, one could simply collect a limited number of readings. Haebarlen *et al.* [3] achieves this goal by dividing the whole area into rooms/cells, thereby limiting the location estimates to room-level granularity. On the contrary, Li *et al.* [2] tries to complete the database using interpolation of readings taken at other training points. Our work has adopted the latter approach. We hold the view that an interpolation-based training approach may stand out when the environment or setup changes. Normally, in such scenarios, the location services may be suspended, while waiting for the creation of an appropriate location fingerprint database that models the change. This procedure is both time and labor intensive. On the contrary, the location system administrator may choose to continue location service provisioning by

performing a rough survey (i.e., taking a few samples) in the changed environment or setup, and fill up the voids in the training set database with the help of interpolation-based techniques. The database may then be augmented incrementally by taking more samples until the location system achieves a reasonable accuracy. Li *et al.* [2] have only used some intuitive guidelines to generate these *fake* training points. In this paper, we have used weighted linear regression in order to obtain a better fit for those *fictitious* training points exploiting spatial similarity [4] of signal strength distribution.

Today, a myriad of devices incorporate multiple wireless technologies; such a trend is expected to thrive in the near future as well. Subsequently, there may be a substantially large number of APs from different technologies serving these devices. If we consider all the different technologies' signals collectively to denote a location's signature, many APs' signals need to be considered for any particular location. Prior works [5] have shown that increasing the number of APs to denote a particular location's signature does not necessarily increase the accuracy monotonically. It may be wise to use a smaller number of *good* APs to denote signature, as it reduces the storage requirements and computational overhead. In this paper, we have devised some simple criteria to distinguish *good* APs, which we term as *anchors*. We claim that the consideration of these anchors' signals alone would achieve similar accuracy to a system that uses all APs' signals collectively as a signature.

The rest of the paper is organized as follows. In Section II, we provide a brief description of related works. Section III sketches our contributing ideas in the field of fingerprint-based location systems. In Section IV, we present experimental findings supporting our claims. Finally, we depict in Section V the conclusions drawn, and future work.

II. Related Work

Although GPS is the most popular outdoor localization system, it does not work well indoors because its signals are not designed to penetrate most construction materials. The research efforts for indoor localization systems can largely be divided into two main categories:

- Those that rely on specialized hardware (e.g., IR or RF tags, ultrasound receiver) and require extensive deployment of infrastructure solely for localization purpose [6]–[9].
- Those that are built on top of existing infrastructure (e.g., Wi-Fi or Bluetooth networks) and use off-the-shelf wireless networking hardware [10]–[16].

Our research focuses on the second category above, as these systems are gaining popularity due to their ease of integration and cost-effectiveness. In the following, we provide a brief discussion about some existing approaches under this category. Interested readers may refer to [17], [18] for more in-depth discussions.

The second category above mainly depends on location fingerprints; these schemes try to uniquely identify a location based on the perceived signal strengths at that point. This family of localization techniques arose with RADAR [10] mainly because of the unavailability of appropriate radio signal propagation models indoors. It opened the door for many different techniques to be applied for the localization problem. For example, Nibble [11] is one of the first systems to use a probabilistic approach for location estimation. To date, Ekahau's Positioning Engine Software [12] claims to be the most accurate location system based on probabilistic model; they claim a one-meter average accuracy with a short training time. Statistical learning theory [15] and neural networks [16] have also been investigated for localization. Some works [13], [14] also try to aggregate localization data from different technologies (e.g., Wi-Fi and Bluetooth) in order to achieve finer accuracy.

III. Investigated areas for fingerprint-based Localization

In short, our paper addresses the following areas of a typical fingerprint-based location system –

- *Robust Location Fingerprint:* Rather than utilizing absolute signal strength as location fingerprint, we argue both analytically and experimentally that differences of signals perceived at APs would provide a more stable signature for any mobile device irrespective of its hardware used.
- *Fictitious Training Points:* With the help of *proper* interpolation techniques, we show that only a few *real* training samples should be sufficient to achieve a reasonable accuracy for a location system.
- *Anchors:* By intelligently selecting *good* APs (i.e., anchors), a location system can benefit as discussed previously. We have formalized very simple guidelines to denote these anchors in this paper. Future mobile devices will invariably incorporate multiple wireless technologies, thereby, increasing the number of APs servicing them at a particular area. This idea will be even more relevant to that type of scenario.

In Section III-A, we discuss our idea of defining a robust fingerprint for a particular location irrespective of the hardware used at the mobile device. Then, we elaborate on our idea of using simple linear regression techniques to improve localization models with very few training samples in Section III-B. In both cases, we based our analysis upon the shadowing model [19]. We provide some intuitive guidelines in order to choose anchors in Section III-C.

A. Difference of Signals as Fingerprints

Suppose $P_r(d)$ and $P_r(d_0)$ denote the received power of a device at an arbitrary distance d and a close-in

reference distance d_0 from a transmitter, respectively. From the log-normal shadowing model, we get,

$$[\frac{P_r(d)}{P_r(d_0)}]_{dB} = -10\beta \log(\frac{d}{d_0}) + X_{dB} \quad (1)$$

The first part of Eqn. 1 defines the path loss component (β is the path loss exponent) and the second part reflects the variation of the received power at a certain distance ($X_{dB} \sim N(0, \sigma_{dB})$). Eqn. 1 can be rewritten as,

$$P_r(d)|_{dBm} = P_r(d_0)|_{dBm} - 10\beta \log(\frac{d}{d_0}) + X_{dB} \quad (2)$$

Eqn. 2 denotes that, the received signal at a particular location (i.e. treated as location fingerprint traditionally) can be interpreted as an expression of close-in reference power (which incorporates various device specific parameters, e.g., antenna gains) and the path loss and shadowing variation. Depending on the hardware used both at the AP and mobile device, the perceived power at a reference distance, i.e., $P_r(d_0)$ varies – so does the resulting location fingerprint.

We argue that, rather than using absolute signal strength values as location fingerprints, the difference of two APs' received signals from a mobile device can be used to define a more robust signature which we term as *Signal Strength Difference* or *SSD*. To explain analytically, let us assume, $P_r(d_1)$ and $P_r(d_2)$ denote the received signal strength (RSS) at two different APs from a mobile device which are d_1 and d_2 distances away from it, respectively. We assume that, all the APs are of same type, i.e., their hardware (e.g. antennas) used are similar. Consequently, using Eqn. 2, we can write,

For AP_1,

$$P_r(d_1)|_{dBm} = P_r(d_0)|_{dBm} - 10\beta_1 \log(\frac{d_1}{d_0}) + [X_1]_{dB} \quad (3)$$

and for AP_2,

$$P_r(d_2)|_{dBm} = P_r(d_0)|_{dBm} - 10\beta_2 \log(\frac{d_2}{d_0}) + [X_2]_{dB} \quad (4)$$

Combining Eqn. 3 and 4, we obtain,

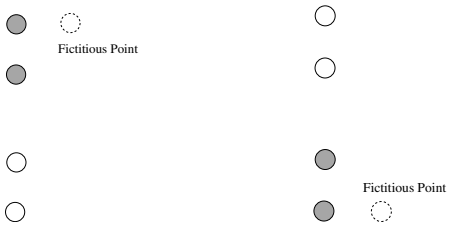
$$\begin{aligned}[\frac{P_r(d_1)}{P_r(d_2)}]_{dB} &= -10\beta_1 \log(\frac{d_1}{d_0}) + 10\beta_2 \log(\frac{d_2}{d_0}) \\ &\quad + [X_1 - X_2]_{dB} \end{aligned} \quad (5)$$

Eqn. 5 denotes SSD's expression which is free from $P_r(d_0)$, thereby, specifies a more robust location fingerprint than absolute RSS.

B. Fictitious Training Points

We know that signal strength varies linearly with $\log(distance)$. In accordance with this testament, Eqn. 1 can further be rewritten in the following way –

$$\begin{aligned}P_r(d)|_{dBm} &= -10\beta \log(d) + P_r(d_0)|_{dBm} \\ &\quad + 10\beta \log(d_0) + X_{dB}\end{aligned}$$



(a) Upper 2 shaded training points contribute heavily

(b) Lower 2 shaded training points contribute heavily

Fig. 1. 4 training points in order to infer 2 different fictitious points. Shaded ones are more important for the corresponding fictitious point because of spatial similarity of signal strength distribution

The preceding equation can be interpreted as, $y = ax + b$ where $y = P_r(d)|_{dBm},\ a = -10\beta,\ x = log(d)$ and we assume, $b = P_r(d_0)|_{dBm} + 10\beta \log(d_0) + X_{dB} = constant$. The standard deviation of RSS at any point in our testbed is measured to be maximum of only 8 dB. Since our RSS fingerprint is an average of many samples, X_{dB} can be considered as constant. Additionally, within a small area which includes the more *important* training points in order to specify a fictitious point, β is likely to have similar characteristics for all the points concerned.

We term *fictitious training points* as those training points in the database that are generated using interpolation from the actual training point sample sets. In order to deduce a fictitious training point, each AP's RSS over the whole localization area is formulated according to the above linear regression equation based on their signatures at the training points. For example, if there are 4 APs, 4 different regression equations will be formed. The unknown parameters, i.e., a and b for each AP are approximated using *weighted least mean square* method. Our target is to minimize $\sum_i w_i(\hat{y_i} - y_i)^2$ where $\hat{y_i}$ and y_i represent the actual and predicted signature respectively for a particular AP at i^{th} training point. We have chosen the weight to be inversely proportional to the distance between a certain fictitious point j and the actual training points i (in our experiments, simply, $\frac{1}{d_{ji}}$). Consequently, we realize that, for each fictitious point, the closer training points contribute more heavily in formulating the APs' regression equations which complies with the spatial similarity of signal strength distribution (See Fig. 1(a) and 1(b)). The main purpose of the weight w_i is to make the contribution of the training points which are closer to fictitious points higher. Note that, in order to obtain a different fictitious point, the regression equations for the 4 APs will be changed. In other words, for inferring each fictitious point, we will be getting 4 different regression equations for the 4 APs everytime.

Once we have approximated the signal patterns over the whole localization area from the APs using the regression model, we would just plug in the distances of the particular fictitious point from the corresponding

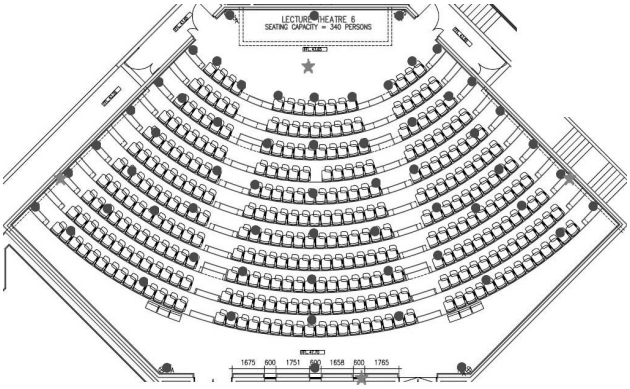


Fig. 2. Our Experimental Testbed

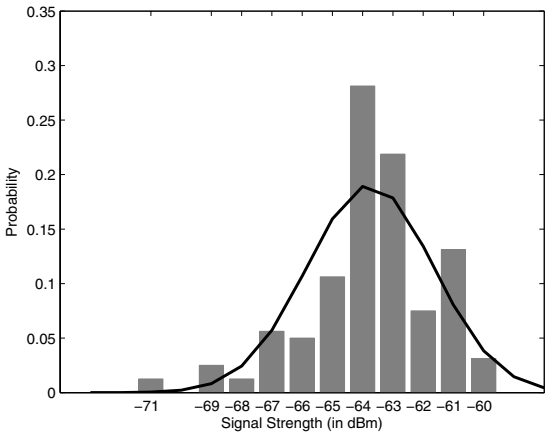


Fig. 3. Histogram of signal strength at a particular training point regarding an AP and its Gaussian approximation

APs in order to obtain its signature.

C. Anchors

Youssef *et al.* [20] used clustering techniques in order to relieve the computational overhead in computing location estimate. They picked locations that see the same k APs with the strongest signal strength values to identify a particular cluster. Since we want to select APs which can be used to differentiate distinct locations based on its signals, our motivation for choosing the k APs or anchors is somewhat different. We term an AP as *anchor* if it shows greater variability of its signals over the whole localization area. We have used two intuitive guidelines in order to choose these anchors:

- *Distinctiveness:* Suppose the mode of the signal strength samples collected at a particular location characterize the location's fingerprint. Let $m_{j_1}, m_{j_2}, \ldots, m_{j_M}$ denote the modes of signal strength samples of the j^{th} AP over the M locations. Among the M modes, assume only l are distinct, $S = \{m_{j_1}, m_{j_2}, \ldots, m_{j_l}\}$. Now, distinctiveness metric for j^{th} AP can be defined as, $dist_j = |S|$. This AP can be considered as anchor if $dist_j \geq \delta$, where δ is a system-defined parameter dependent on the localization area size and the number of different training location grids.
- *Variability:* Another parameter can be taken into account in defining anchors is the variability of an AP's fingerprints over the whole localization area. If mode is chosen to denote location fingerprint as stated in the previous guideline, we have, $\mu_j = \frac{\sum_{i=1}^{M} m_{j_i}}{M}$ and $\sigma_j = \sqrt{\frac{\sum_{i=1}^{M}(m_{j_i} - \mu_j)^2}{M}}$, where μ_j and σ_j represents the average and standard deviation of the j^{th} AP's modes or fingerprints over the whole localization area. Similarly, this AP can be categorized as anchor if $\sigma_j \geq \gamma$ where γ again is a location system dependent threshold.

IV. Experimental Study

In this section, we first describe our experimental testbed and data collection process. Then, we proceed to provide our experimental results and findings.

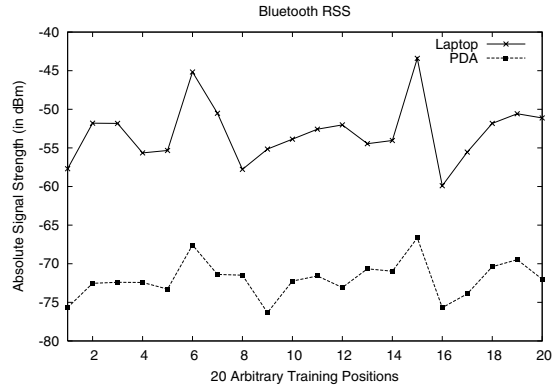
A. Testbed Setup

Our experimental testbed is located inside a lecture theater of our school which spans over an area of $540\ m^2$. We have used four Aopen MP945 Mini PCs to serve as our access points which are placed near the ceilings. The locations of these APs are shown in Fig. 2, marked as stars while the training points are indicated by dots. Each MP945 is installed with Aopen WN2302A mini PCI WLAN adapter in order to passively detect Wi-Fi devices and measure their RSS. They are also incorporated with BT-2100 Class 1 Bluetooth adapters which keep on scanning for Bluetooth packets by issuing inquiry periodically.

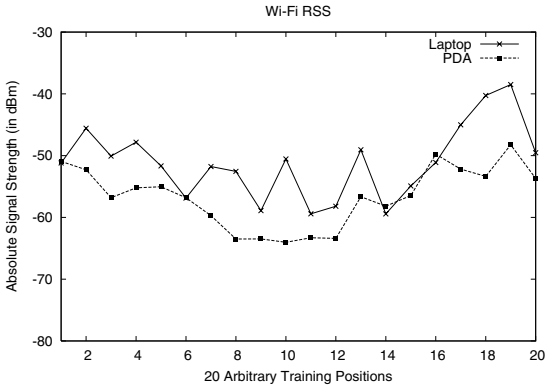
Each Mini PC or AP is connected to our school's intranet for communicating with the server by means of a wired LAN connection. All our mini PCs run SuSe 10.1 Linux distribution with the latest libpcap libraries [21] and BlueZ protocol stack [22].

B. Data Collection Procedure

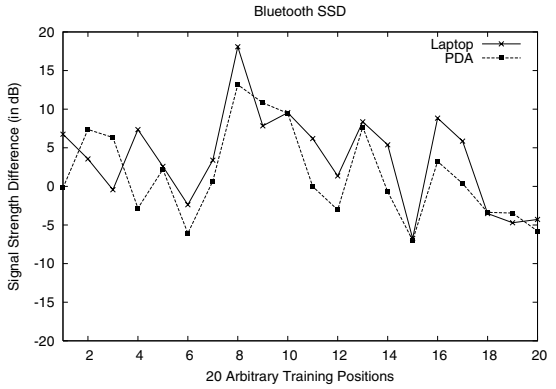
In our testbed, there are 62 training points or grids. The training process starts by placing the mobile device at a particular training point. Since a location system which requires little participation from the mobile device is more desirable, our APs collect RSS information. The WLAN device at the mobile device sends probe request continuously for some time period in order to gather enough packets at the APs listening, while the APs issue Bluetooth inquiry from time to time which the mobile device responds to. In either cases, the packet information is immediately transferred to our central server database. Our Bluetooth adapters provide absolute RSS metric which we have used to denote a location's fingerprint regarding Bluetooth technology since other signal strength values (e.g., relative RSSI, link quality



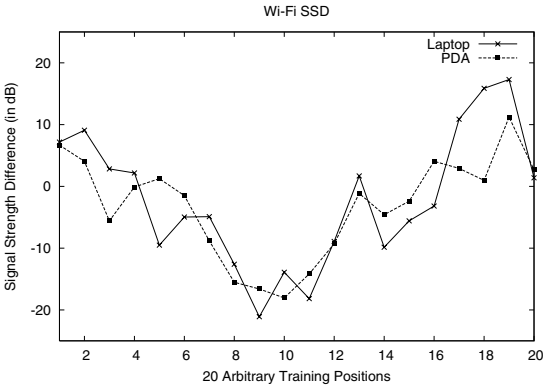
(a) Absolute Signal Strength perceived at a Bluetooth AP



(b) Absolute Signal Strength perceived at a Wi-Fi AP



(c) Signal Strength Difference between 2 Bluetooth APs



(d) Signal Strength Difference between 2 Wi-Fi APs

Fig. 4. RSS and SSD considering 2 different devices (e.g., Laptop and PDA) incorporated with both Bluetooth and Wi-Fi

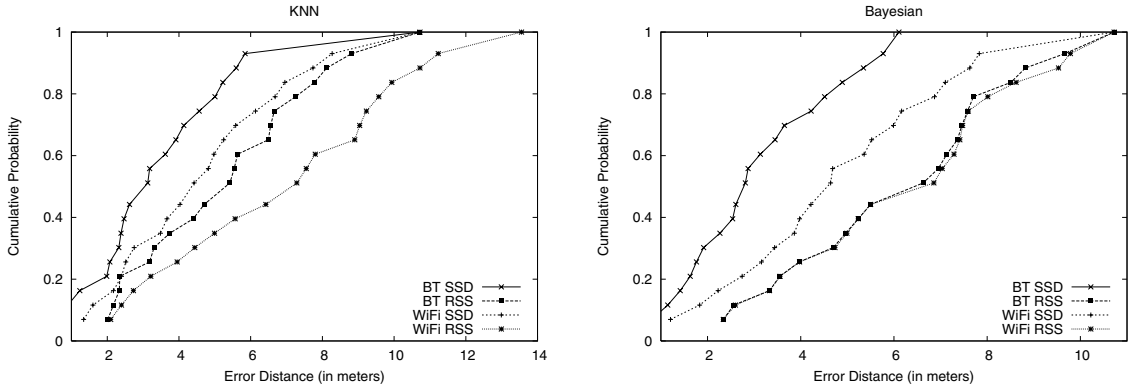
etc.) made available in Bluetooth Core specification [23] have already been proven unsatisfactory for localization purpose [13]. Finally, we have chosen 44 testing points which are completely different from our training locations. The central server is responsible for calculating the location estimate during the testing phase.

C. Experimental Results and Findings

First, we list the assumptions we have made corresponding to our experiments performed:

- In our paper, whenever we have used RSS as location fingerprint for certain experiments, we assumed it to be normally distributed. Though some works defy this phenomenon, others lend support to it [4]. Our experimental results also suggest it to be a reasonable approximation – we have not achieved significant improvement considering a histogram representation of RSS. Fig. 3 shows RSS distribution at one particular point for a certain AP and its Gaussian approximation curve.
- We have chosen two well-known algorithms in localization literature, namely, KNN and Bayesian probabilistic model in order to test our ideas. The reason behind selecting these two well-known algorithms is, our purpose is to show that the ideas are quite generic and can be productive irrespective of the choice of algorithms. We chose the value of K empirically for KNN algorithm similar to prior works [10]. While applying Bayes formula, the prior probabilities are assumed to be uniformly distributed.
- In order to apply probabilistic models, one assumption which has widely been used is the independence of RSS values from different APs. This assumption is justifiable for a well-designed network where each AP runs on a non-overlapping channel. Kaemarungsi and Krishnamurthy [4] performed experiments in order to evaluate the correlation factor among the APs' RSS values in presence of interference and thereby, strengthened this claim. We also adopted their vindication.

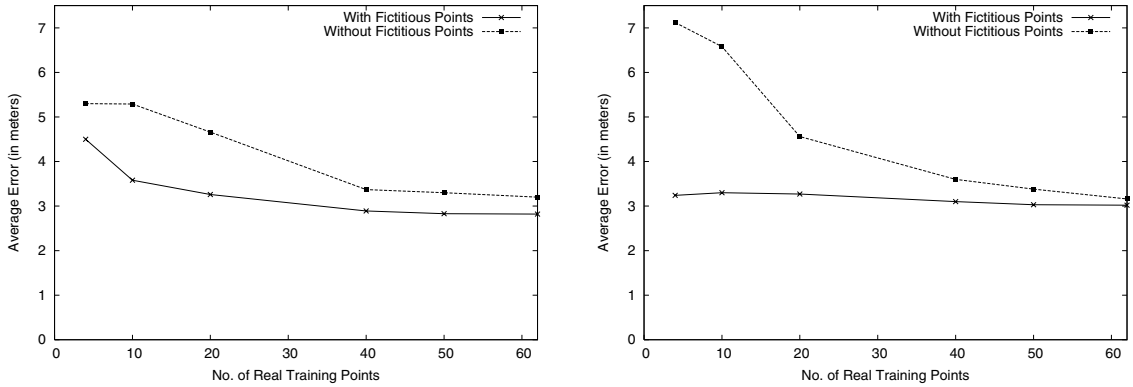
1) Justification of SSD as robust fingerprint: For this experiment, we have selected two different devices (e.g., Laptop and PDA) and measured their signal strengths at the APs. Our Laptop is installed with an Intel PRO/Wireless 3945 ABG Mini PCI WLAN adapter whereas the WLAN card used in our PDA is Samsung SWL-2455 802.11b. Similarly, our PDA has integrated Class 2 Bluetooth chip where a Class 1 Bluetooth USB adapter has been plugged into the Laptop during



(a) KNN's performance w.r.t. various location fingerprints

(b) Bayes' performance w.r.t. various location fingerprints

Fig. 5. Comparison of RSS and SSD as location fingerprint for both Bluetooth and Wi-Fi considering KNN and Bayesian algorithms



(a) KNN's performance with and without fictitious points

(b) Bayes' performance with and without fictitious points

Fig. 6. KNN and Bayesian algorithm's performance corresponding to various number of *real* training locations. A fixed number of fictitious training points are generated in each case.

the experiments. We have picked 20 random training points and stationed ourselves with the device at those locations and collected enough samples at the APs for both devices. Fig. 4(a) and 4(b) are drawn with the RSS readings at a particular AP whereas Fig. 4(c) and 4(d) plot the difference between the RSS values seen at two different APs.

From Fig. 4(a) and 4(b), it is apparent that, absolute signal strength perceived at a certain AP varies quite significantly for the two devices. This has repercussion in the form of fingerprint being quite different when different mobile devices are used during training. Most works perform their training and testing phase with the same device, thereby, shielding the adverse effect of this phenomenon. On the contrary, SSD does not quite suffer from this effect, thereby, providing a more robust fingerprint as seen in Fig. 4(c) and 4(d). This readily complies with our analysis in Section III-A. We further notice from Fig. 4(c) that SSD regarding Bluetooth tends to be more robust which will be further verified by our later results.

2) Comparison of SSD and RSS as Location Fingerprint: As illustrated in Fig. 5(a) and 5(b), it can be seen that, location system built upon SSD outperforms its RSS counterpart in case of both Bluetooth and Wi-Fi. Furthermore, we also see that, Bluetooth SSD based systems perform better than location systems utilizing Wi-Fi SSD as anticipated in the previous experiment. There can be 6 different pairs of 4 APs (for both Bluetooth and Wi-Fi) which may be exploited to deduce 6 SSD values per location. But through our experiments, we have seen that, only 3 such values are sufficient in order to achieve similar performance compared to the scenario when considered all 6. Consequently, our SSD vector consists of only 3 elements for both Bluetooth and Wi-Fi which is 1 element less than its RSS vector counterpart.

3) Importance of Fictitious Training Points: In Section III-B, it was argued that applying proper interpolation techniques could enhance an under-trained location system's accuracy immensely. In that regard, our simple linear regression-based method performs very well as manifested in Fig. 6(a) and 6(b). We can see

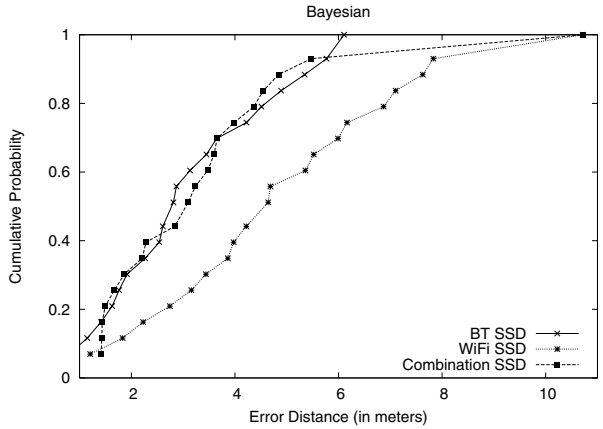


Fig. 7. Considering 4 BT APs is similar to taking into account all 8 (4 BT + 4 Wi-Fi) APs combined

that, gathering training samples at only 20 locations and generating fictitious training points based on them, actually outperforms a location system with as many as 62 training points. For producing Fig. 6(a) and 6(b), a fixed number of fictitious points are realized for each *real* training point case. Then, SSDs are calculated utilizing both types of training points (i.e., real and fictitious). Finally, both KNN and Bayes algorithms are fed these SSDs for localization purpose. For this experiment, we have only included graphs considering Bluetooth SSDs – a location system comprised of Bluetooth APs only. Considering Wi-Fi APs also showed similar performance enhancement in our experiments.

4) Anchor Experiment: Based on our intuitive guidelines for selecting anchors as discussed in Section III-C, we find that, Bluetooth APs are more likely to be picked as anchors in our case. Fig. 7 reveals that considering only 4 Bluetooth APs (i.e., anchors) performs almost similar or even better compared to a location system utilizing all 8 APs available. For this experiment, both the *distinctiveness* and *variability* metric were calculated for all 8 APs and then 4 were chosen.

V. Conclusions and Future Work

In this paper, we addressed some interesting issues regarding fingerprint-based location system and obtained favorable results. Based on our analysis and experimental findings, the following conclusions can be drawn:

- SSD provides a more robust location fingerprint than traditional RSS regarding radio propagation. Our analysis as well as experimental results verify this claim.
- Adopting appropriate interpolation technique can go a long way in solving the drawbacks suffered by an under-trained location system as vindicated by our analysis and results. Prior works [2] have indicated that when enough samples are taken over the whole localization area, the gain using interpolation techniques is not significant. Our results show similar trend as revealed in Fig. 6(a) and 6(b). In addition, it can be seen that, a moderate testbed size like ours would require 62 or more *real* training points where samples need to be collected in order to approach reasonable accuracy. This makes our technique necessary for testbed of large or fair size in order to shorten training period and also to reduce labor and cost.
- It has been proved in some works [5] that increasing the number of APs do not necessarily increase the localization accuracy monotonically. So in a setting of many APs, it is convenient to find a subset of APs which we denote as anchors. Selection of these APs certainly have impact on localization accuracy since from Fig. 7, we see that, 4 Wi-Fi based location system's performance falls well short of its Bluetooth counterpart. Our guidelines guaranteed us to select the Bluetooth APs, thereby, ensuring similar accuracy compared to the overall system.
- Because of Bluetooth's inappropriate signal strength parameters (e.g., relative RSSI, link quality etc.) used for localization and due to lack of widespread availability of Bluetooth networks, no work has been successful in designing a reasonable Bluetooth location system so far. Through the choice of SSD as location fingerprint, we actually find Bluetooth outsmarting Wi-Fi in all scenarios for our experiments.

In summary, we tried to arrive at a robust location fingerprint definition analytically and verified it experimentally as well. We also devised a way through simple linear regression techniques to facilitate under-trained location systems. Moreover, we considered multiple wireless technologies and formulated some simple intuitive ideas to form a subset of *good* APs among the APs serving their respective technologies. In the following, we list some important future directions that we foresee:

- SSD performed well as location fingerprint in our experiments. Since we have only tested it in our own testbed of moderate size, it should be verified by performing experiments in testbeds with different setup and size in order to be more conclusive.
- For generating fictitious points, we have used linear regression model under some simplified assumptions. Other complex propagation models may even be more suitable regarding these types of interpolation techniques.
- We only had provided some intuitive guidelines in order to choose anchors. A theoretical approach in choosing the right number of anchors and which APs to select as anchors within certain constraints might be interesting.

- Localization systems dependent on Bluetooth certainly require more investigation. We obtained promising results regarding Bluetooth while previous works [13], [14] either provide discouraging results or require the aid of additional wireless technologies (e.g., Wi-Fi).
- Because of the proliferation of mobile devices incorporated with multiple wireless technologies and many APs serving the same area now, cluster-based approach [20] would be interesting prospect for future. More research should be performed on how to divide a localization area into clusters based on the myriad types of APs.

VI. Acknowledgments

The research reported in this paper was supported by the Ministry of Education of Singapore, AcRF Tier 1 funding, under Grant No. R-263-000-320-112 and R-263-000-320-133.

References

[1] P. Tao, A. Rudys, A. M. Ladd, and D. S. Wallach, "Wireless LAN location-sensing for security applications," in *Proceedings of the second ACM Workshop on Wireless Security (WiSe '03)*, San Diego, CA, Sept. 2003, pp. 11–20.

[2] B. Li, J. Salter, A. G. Dempster, and C. Rizos, "Indoor positioning techniques based on wireless LAN," in *1st IEEE Int. Conf. on Wireless Broadband & Ultra Wideband Communications*, Sydney, AUS, Mar. 2006.

[3] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki, "Practical robust localization over large-scale 802.11 wireless networks," in *Proceedings of the 10th annual international conference on Mobile computing and networking (MobiCom '04)*, Philadelphia, PA, 2004, pp. 70–84.

[4] K. Kaemarungsi and P. Krishnamurth, "Properties of indoor received signal strength for WLAN location fingerprinting," in *1^{st} Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04)*, San Diego, CA, 2004, pp. 14–23.

[5] K. Kaemarungsi and P. Krishnamurthy, "Modeling of indoor positioning systems based on location fingerprinting," in *Proc. of the 23^{rd} Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM'04)*, Mar. 2004, pp. 1012–1022.

[6] R. Want, A. Hopper, V. Falcão, and J. Gibbons, "The active badge location system," *ACM Trans. on Information Systems*, vol. 10, no. 1, pp. 91–102, Jan. 1992.

[7] A. Ward, A. Jones, and A. Hopper, "A new location technique for the active office," *IEEE Personal Communications*, vol. 4, no. 5, pp. 42–47, Oct. 1997.

[8] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proc. of the 6^{th} Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, Boston, MA, Aug. 2000, pp. 32–43.

[9] N. Priyantha, A. Miu, H. Balakrishnan, and S. Teller, "The cricket compass for context-aware mobile applications," in *Proceedings of the 7^{th} Annual International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001, pp. 1–14.

[10] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proceedings of the 19^{th} Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Tel Aviv, Israel, Mar. 2000, pp. 775–784.

[11] P. Castro, P. Chiu, T. Kremenek, and R. R. Muntz, "A probabilistic room location service for wireless networked environments," in *Proceedings of the 3^{rd} International Conference on Ubiquitous Computing (UbiComp '01)*, Atlanta, GA, Sept. 2001, pp. 18–34.

[12] Ekahau. [Online]. Available: http://www.ekahau.com/

[13] D. Pandya, R. Jain, and E. Lupu, "Indoor location using multiple wireless technologies," in *Proc. IEEE PIMRC*, Beijing, China, Sept. 2003, pp. 2208–2212.

[14] Y. Gwon, R. Jain, and T. Kawahara, "Robust indoor location estimation of stationary and mobile users," in *Proc. of the 23^{rd} Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM'04)*, Mar. 2004, pp. 1032–1043.

[15] R. Battiti, M. Brunato, and A. Villani, "Statistical learning theory for location fingerprinting in wireless LANs," Universita di Trento, Dipartimento di Informatica e Telecomunicazioni, Tech. Rep. DIT-02-0086, Oct. 2002.

[16] R. Battiti, T. L. Nhat, and A. Villani, "Location-aware computing: a neural network model for determining location in wireless LANs," Universita di Trento, Dipartimento di Informatica e Telecomunicazioni, Tech. Rep. DIT-02-0083, Feb. 2002.

[17] J. Hightower and G. Borriella, "Location systems for ubiquitous computing," *IEEE Computer*, vol. 34, no. 8, pp. 57–66, 2001.

[18] K. Pahlavan, X. Li, and J. Maleka, "Indoor geolocation science and technology," *IEEE Communications Mag.*, vol. 40, no. 2, pp. 112–118, 2002.

[19] T. S. Rappaport, *Wireless Communications – Principles and Practice*. Prentice Hall, 1996.

[20] M. A. Youssef, A. Agrawala, and A. U. Shankar, "WLAN location determination via clustering and probability distributions," in *Proceedings of the 1^{st} IEEE International Conference on Pervasive Computing and Communications (PERCOM '03)*, Mar. 2003.

[21] Libpcap, "The libpcap project." [Online]. Available: http://sourceforge.net/projects/libpcap/

[22] BlueZ, "Official linux bluetooth protocol stack." [Online]. Available: http://www.bluez.org

[23] Bluetooth, "Bluetooth core specification v1.2." [Online]. Available: https://www.bluetooth.org/spec/