WLAN Location Sharing through a Privacy Observant Architecture

Kavitha Muthukrishnan, Nirvana Meratnia, Maria Lijding, Georgi Koprinkov and Paul Havinga

University of Twente, Faculty of Computer Science
Computer Architecture Design and Test for Embedded Systems group
P.O.Box 217, 7500 AE, Enschede, The Netherlands
{k.muthukrishnan, n.meratnia, g.t.koprinkov, m.e.m.lijding, p.j.m.havinga}@ewi.utwente.nl

Abstract— **In the last few years, WLAN has seen immense growth and it will continue this trend due to the fact that it provides convenient connectivity as well as high speed links. Furthermore, the infrastructure already exists in most public places and is cheap to extend. These advantages, together with the fact that WLAN covers a large area and is not restricted to line of sight, have led to developing many WLAN localization techniques and applications based on them. In this paper we present a novel calibration-free localization technique using the existing WLAN infrastructure that enables conference participants to determine their location without the need of a centralized system. The evaluation results illustrate the superiority of our technique compared to existing methods.**

In addition, we present a privacy observant architecture to share location information. We handle both the location of people and the resources in the infrastructure as services, which can be easily discovered and used. An important design issue for us was to avoid tracking people and giving the users control over who they share their location information with and under which conditions.

I. Introduction

We all have occasionally experienced being alone in a foreign territory. Naturally, it had come to our mind it would have been nice if we were accompanied by a trustworthy native person who knows a great deal about the area, places worth visiting, and how to find our way and our points of interest, etc. As unrealistic as it may sound, that is exactly what this research aims at, i.e, building a mobile guide to (temporarily) be your best friend when you are attending a conference.

The idea is built on top of already existing *wireless campus* at the University of Twente (UT), in the Netherlands. Equipped with 650 individual wireless network access points, each of which having a range of about 100 meters. Spread over 140-hectare campus, UT offers its staff, students, as well as its visitors, i.e., anyone with a desktop, laptop, handheld or wireless fidelity (Wi-Fi) devices to wirelessly access the university's network and the Internet from everywhere on the campus [1]. Availability of such infrastructure is a strong driving force towards building useful applications as well as practical use cases upon. One of such use cases is our conference assistant, i.e., FLAVOUR (Friendly Location-aware conference Assistant with priVacy Observant architectURe), which was provided for the first time to the participants of the 4^{th} Annual Conference on Scalable Vector Graphics (SVGopen 2005) taking place in August 15-18 2005 at UT.

Appearing under different names, the most basic and popular services for conference participants can be grouped into the following three categories:

1) *Finding fellow attendees*. Colleagues attending the conference may want to participate in many of the parallel sessions they are interested in. Thus, by locating colleagues who share the same interests, one can check whether they join one of the other presentations and can be updated about him. People also want to find colleagues and friends during the conference in order to have lunch or coffee together. While making this service available, we do not want to provide an anonymous tracking functionality by which conference participants can be tracked without being aware of it. Instead, the attendees themselves decide who can be aware of their location. They also can determine when and for how long other people should be given access to this information.
2) *Locating and using resources*. Easily finding out about available resources is always useful. Some resources are as simple as location of static points of interest, such as the restaurant, the conference rooms where the talks are taking place, Internet access rooms and coffee machines. We also want to provide easy use of resources available in the infrastructure such as printers. The users can then seamlessly send documents to print and be shown

0-7803-9575-1/06/$20.00 ©2006 IEEE

the location of the printer that has their documents. We also aim at providing additional information about the resources, e.g. the current presentation in a certain room or availability status of computers in the Internet access room.

3) *Receiving messages and notifications*. Instead of using an announcement board, conference organizers can use a messaging mechanism to reach all attendees. This is handy for organizational announcements, such as changes in schedules, session cancellation or diversions, as well as social events announcements.

Following Langhereich's guidelines [2] we have made privacy an important design issue of our architecture and not considered it as an afterthought as in most Ubiquitous Computing projects [3]. There are two main design issues that make FLAVOUR privacy observant. On the one hand, it adheres to the widely accepted notion of privacy formulated by Westin in 1967 that "privacy is the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others" [4]. On the other hand, the location is determined by software controlled by the users, which either runs completely on their mobile devices or partly on their mobile devices and partly on the infrastructure in a distributed manner. Thus, there is no centralized services that track the users' location.

We base our localization method on WLAN for several reasons. Firstly, the infrastructure already exists in most public places such as universities, corporations, airports, shopping malls. Furthermore, IEEE 802.11 based WLANs have seen immense growth in the last few years, and we believe this trend will continue because WLAN provides not only convenient connectivity but also a high speed links up to 11Mbps (802.11b). Since the wireless network infrastructure already exists, localization can be done by a software-only method eliminating the need for additional hardware. Secondly, when compared to other radio techniques like bluetooth or RFID, the range covered by WLAN is more, reaching approximately 50-100m. Thirdly, it is ubiquitous because wireless networks are being deployed at all important places. Finally, there are no line of sight restriction when using WLAN. Additionally, using WLAN the users can determine their location in a local manner, without having to sacrifice their privacy.

The rest of the paper is organized as follows. Related work on conference assistants and WLAN localization are addressed in Section II. Section III represents our proposed privacy observant architecture to enable location sharing, which in turn is explained in Section IV. Various metrics for evaluating WLAN localization is addressed in Section V, which is followed by the localization in FLAVOUR explained in Section VI. Our experimental results are presented in Section VII before concluding the paper in Section VIII.

II. Related Work

In this section, most relevant state-of-the art on both conference assistants and WLAN localization methods are presented.

A. Conference assistants

In recent years, some attempts have been made to offer various value-added services to conference attendees. The central theme in these systems is either the ability to track individual attendees as they move around or to detect when they interact with each other.

The goal of SpotMe [5] is to provide support in conferences. As far as location awareness is concerned, the system mainly provides a radar functionality. SpotMe lets participants in a conference *(i)* know who is in a radius of 30 meter around them, *(ii)* know if a certain person is near, and *(iii)* be notified when a searched person or a person sharing the same interests approaches. SpotMe requires participants to carry a special cell phone-size device as interface, to identify themselves, and to provide their location to the system. Clearly, SpotMe is not privacy observant, as the participants are not aware of who is seeing their location and information. Moreover, they are continuously being tracked unless their devices are off.

The IntelliBadge system, which was showcased at IEEE supercomputing conference in the year 2002, implements location tracking through proximity to RF location markers installed at the points of interest [6]. All the user services are built around tracked location information and a priori knowledge about the participants and the conference events.

The Meme Tags project [7], used electronic name tags capable of exchanging short messages (memes) via infrared (IR). The tags were also capable of storing information about the interaction between people wearing the tags as well as sharing this information with a centralized database. Consequently, the cumulative data was shown on large displays called Community Mirrors.

CharmBadge [8] uses IR-based tags programmed with participants' individual business card information. This information is exchanged between participants as they interact with each other and the interaction is logged and subsequently uploaded to a private website accessible by each user. The system does not provide data to the users in real-time, nor does it provide location information.

nTag [9] uses semi-passive Radio Frequency IDentification (RFID) tags operating in the UHF band that enable conference organizers to record how many people attend certain sessions, or visited certain areas of an exhibition floor. In addition, using the system conference participants can exchange information about their interests and preferences via their tags whenever/wherever they meet.

Our focus differ from the above-described systems in terms of the technology used *-WLAN(RF)*, as it uses the existing WLAN infrastructure to enable conference participants to determine their position without the need of a centralized system. Therefore, the participants cannot be tracked. In addition, the users can decide who to share their location with, imposing the privacy rules that they see fit (e.g. time restrictions or frequency of updates). Additionally, the location of the participants is represented as a service, which can be easily discovered and used.

B. WLAN localization

RADAR is a RF-based location system, which is mainly used to track users inside the buildings [10]. It operates by recording signal strength information from multiple base stations. In addition a centralized system is used to perform triangulation and consequently to compute the location of the user. The RADAR system combines empirical measurements with signal propagation modelling to determine the users' location. The Users' location can also be computed by probabilistic approaches [11] or neural network model [12]. Joint clustering [13] and Bayesian Networks [14] are similar to RADAR. They all use a training session to get many fingerprints and using them they try to predict the location. This process is often referred to as *finger printing (FP)*. The main disadvantage of these methods is their lack of scalability due to the need for extensive calibration.

Ekahau positioning system [15] is a software tool, which is able to locate targets and provides the coordinates (x,y,z) corresponding to each client. The main positioning module is run on the server or a PC. It gives an accuracy of about 1m, however it requires a considerable calibration effort.

Place lab [16] is a new initiative developed by Intel, which allows commodity hardware clients like laptops, PDAs and cell phones to locate themselves by scanning for radio beacons such as 802.11 access points, GSM cell towers and fixed bluetooth devices. It does not involve much calibration, as information about the access points and GSM cell towers are collected through *war driving*. It has been demonstrated only for outdoor environments where radio propagation is not harsh, reporting accuracy of 13 to 20m [16]. It maintains privacy by computing the locations of the users at the client device. PlaceLab does not provide a mechanism to share locations. However, it is being integrated into different systems such as Active Campus [17] providing that functionality. We are using the Spotter functionality of PlaceLab to query the network driver.

The problem in these aforementioned state-of-the-art is that the localization methods either involve too much calibration efforts or give too little accuracy. So we set our objective to reduce the calibration effort and offer better accuracy.

III. FLAVOUR ARCHITECTURE

In this section, we first identify the following issues as high level technical requirements for the system:

- the users do not have to be equipped with specialized hardware,
- the system should be able to determine the users' location indoors as well as outdoors with a reasonable accuracy and the transition should be transparent to the user,
- the system should not track the user, therefore, the users should be able to determine their location locally,
- the users should decide who has access to their location information, when, and for how long,
- keeping the users location private should not restrict them from using the services provided, and
- the system's user interface should be lean, because of shortage of resources on the users' mobile devices.

To meet the first three requirements we have decided to base our system on the use of the WLAN infrastructure as devices equipped with a WLAN card (e.g. laptops and PDAs) can determine their location without any additional hardware, both indoors and outdoors. Additionally, the users can determine their position locally, without disclosing their position to a centralized system. Furthermore, they can share their locations with other participants in a peer-to-peer fashion.

The participants fully control the application that computes and shares their location. Part of this control is to decide how and with whom they want to share their location information. The participants offer their location information as a *location service*. The interface of the service provides both a *location request* and a *location subscription*. The service is announced in a *Lookup Service* so that the other participants can easily find it and, if allowed, use it. It is important to note that

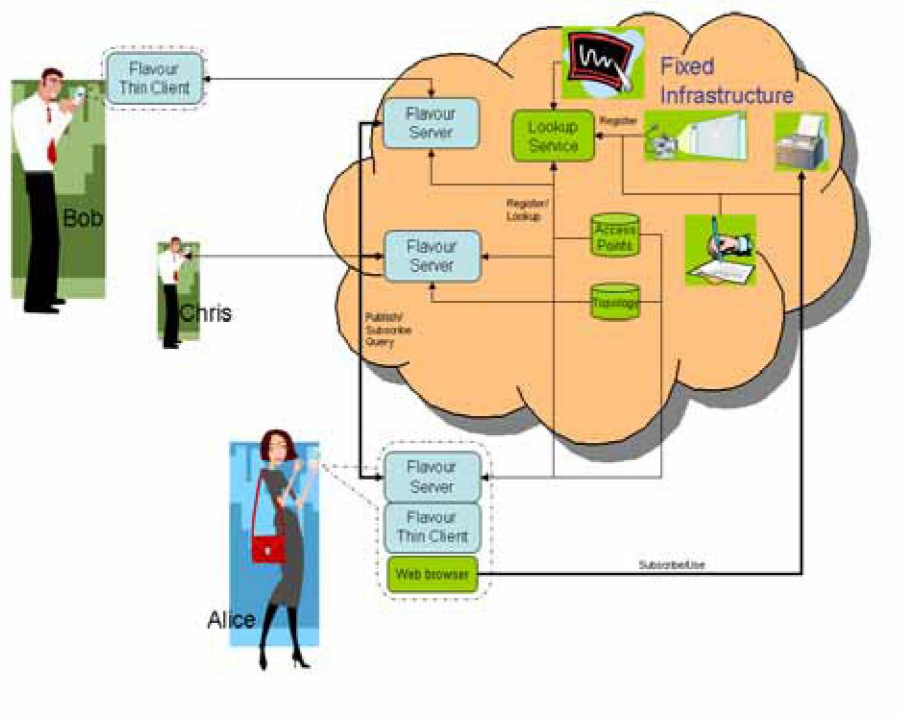


Fig. 1. High level view of the system architecture

the *Lookup Service* only announces that the services exist and provides a way to access them. It does not need to know where the participants are and whether they are allowed to use the services.

It can clearly be seen that FLAVOUR is a service-oriented architecture. All the services can be discovered through the *Lookup Service*. Figure 1 shows a high level view of our proposed architecture for the system.

The information about the access points is stored in a database, which is used by FLAVOUR to compute the location of the participants. Another source of information to be used is the conference venue topology that is stored as geo-referenced maps. Using these maps, the participants are able to visualize their location, and the location of other people and resources available on the infrastructure on the venue footprint.

Some important services offered by the system to all the participants are a *public key authority*, and a *message board*. Additionally the conference organization can also offer some services as a printing service and a remote control of devices (e.g. overhead projectors). The *public key authority* stores a public key for each participant, which is provided by the participant when registering and is the counterpart of the private key he will use to 'sign' messages in order to identify himself.

To meet the last requirement we have created a thin client that has to run on the participant's mobile device, while the server part can either run on the mobile device or on the 'infrastructure'. By infrastructure we mean a server which does not need to be switched off or sent to sleep because it is running on batteries and has a permanent network connection. The conference organization provides those servers, but the user may prefer to run the software in a trusted server connected to the Internet, for example a server back at his office. In the example illustrated in Figure 1, Bob and Chris run the *Flavour Server* on the fixed infrastructure, while Alice runs it on her mobile device. As shown, they are subscribed to each others location services. Alice is also using the print service to print some web pages.

The advantage of running the *Flavour Server* on the infrastructure is that the location service can still be provided even if the client's device is off. The time-stamped location provided will be the last location in which the user's device was on. Furthermore, in this manner nothing can be concluded from the existence of the participant's location in the *Lookup service*, because his location service is always available. On the other hand, the participants may not trust the conference organizers or may not be interested in sharing their location when they are off-line, and, thus, run the *Flavour Server* on the mobile device. At present we cannot guarantee absolute privacy of the data when the *Flavour Server* runs on the infrastructure, as in principle it is possible that the administrator of the system hosting the software 'spies' on the user. However, we have made spying on the participants difficult, as the software does not provide the system administrators any information. In the future we are planning to be able to run the *Flavour Server* both on the mobile device and on the infrastructure or to be able to migrate it easily.

As shown in Figure 2 the functionality provided by FLAVOUR can be divided into:

- **Location Sharing:** The participants can provide their location to other participants and can be aware of other participants location. There are two mechanisms to share location information: *publish/subscribe* and *request*. With the former the publisher sends updates whenever the location of the participant changes in a significant manner, while with the latter the information is provided as a reply to a (one time) request. In both cases the *Privacy Guardian* decides if the request should be rejected or accepted, and if accepted under which conditions (e.g. granularity, update frequency, duration). The location sharing functionality is discussed in more detail in Section IV.
- **Localization:** In order to determine the user's location the *Spotter* measures the signal strength of all the access points it hears. The *Spotter* sends those measurements to the *Localizer*, which in turn will use them to compute the user's location. The localization functionality is further described in Section VI.
- **Visualization:** The participants can visualize their location, as well as the location of other participants and points of interest on an SVG map using the *Map Viewer*. The *Renderer* composes SVG maps using the topology of the venue and points of interest, the coordinates of the user provided by the *Localizer*, and the location of other participants provided by the *Location Subscriber*. Figure 3 illustrates a snapshot of the FLAVOUR interface.
- **Message Board:** The conference participants can receive and send messages to the message board. The messages from the message board are either sent to all the participants or to particular groups, for example the people giving a presentation on specific session, or all people who registered themselves for a social event. The participants can also send messages to the message board either to all or to certain groups. Although, not yet implemented, there should be some control about what is being published in the message board. The *Message Board Subscriber* handles the subscriptions of the user to the message board and gets the messages. If the mobile device is unavailable (e.g. switched off) it keeps the messages and transmits them to the *Message Board Client* when it becomes available. By keeping the subscription even when the client is unavailable, we do not disclose unnecessary information to the organization about the status and location of the participant.

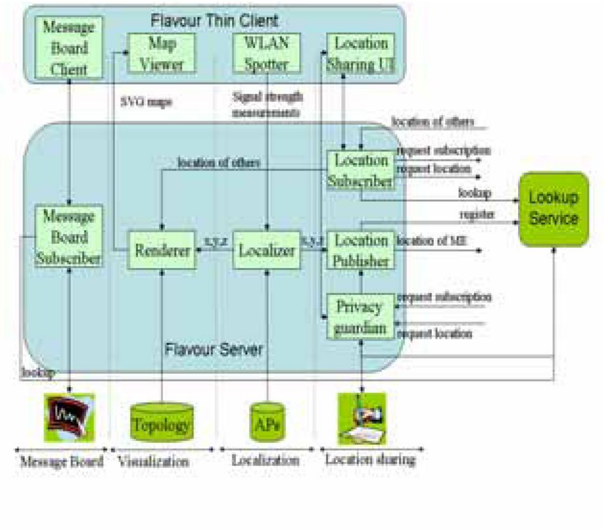


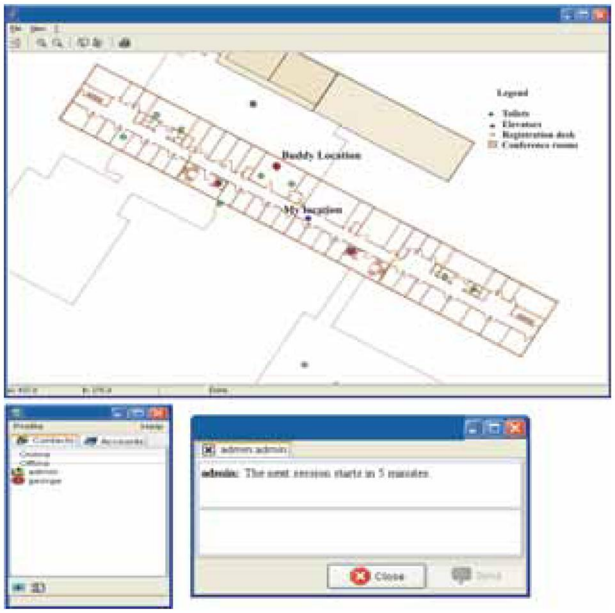
Fig. 2. Components of FLAVOUR

IV. Location Sharing

A very important issue for sharing location is privacy. In FLAVOUR we want each participant to decide what location information can be disclosed and to control when and how it is disclosed. Furthermore, the organization does not have access to the location of participants, unless the participants themselves allow the organization to subscribe to their location or allow the organization to request their location.

The *Lookup service* provides an entry for every person that registers to the conference. The information in the *Lookup service* is the participant's name, affiliation and a pointer to his *Flavour Server*. This is nothing more than the standard information that at present is distributed to the participants of a conference on paper or on CD-ROM. Thus, we are not violating the participants privacy more than is nowadays done.

The basic interface provided by FLAVOUR to other participants is:



admin: The next session starts in 5 minutes

Fig. 3. Snapshots of FLAVOUR interface

- getLocation(Requester, Reason): One time request for the location of the user.
- subscribeToLocation(Requester, Reason): Subscribe permanently (i.e. during the conference) to the location of the user.
- subscribeToLocation(Requester, Reason, TimePeriod): Subscribe during a certain period to the location of the user for a given period.

The reply to a request for subscription may restrict the subscription to a shorter time period and additionally put restrictions to the accuracy of the provided location and frequency of the updates. In all cases the request may be rejected.

The *Privacy Guardian* uses the identity of the *Requester* to decide if the service requested should be provided and with what restrictions. On the one hand, the *Privacy Guardian* checks the identity of the *Requester* (if he is who he says) using a challenge-response protocol. For this purpose it uses the *public key authority* service provided by the system that stores the public keys of the participants. In order to decide who can access the services and under which conditions, the user can create a buddy list using the *Location Sharing User Interface* and assigning access rights. If a request comes in from a person not in the list, the *Privacy Guardian* can ask the user for action through the *Location Sharing UI* using a similar mechanism to a cookie blocker that provides options as *'allow once'*, *'allow during conference'*, *'block once'*, *'block always'*, or set explicit time restrictions and intervals for updates. In the future we will add the capacity to set the accuracy of the location provided as well. The *Privacy Guardian* stores the reply from the user to decide what to do next time a request from the same person arrives.

All arriving requests and their replies are logged by the *Privacy Guardian*. In this way the user can afterwards analyze who requested his location and why by looking at the provided *Reason*. At present the *Privacy Guardian* does not have the capacity to analyze the given *Reason*, instead it either just passes it on to the user to decide to accept or reject the request, or simply logs it for future analysis. Thus, we rely on normal social control to prevent abuse of the system (see [18] for a discussion on the subject). The *Privacy Guardian* also has tools to let the user analyze the log and to provide warnings in case of possible abuses, for instance if a participant inquires for other participant's location very frequently. The frequent inquiring may be justified by the given *Reason*, otherwise the participant may find frequent inquiring a breach of trust and consequently revokes or restricts the requester's access rights.

Allowing individual requests is more privacy preservant that allowing subscriptions. As by allowing subscriptions the user cannot see when the subscriber is really looking at his location. Thus, basically he is allowing to be tracked. Although the study performed on Active Campus by Griswold et al. [17] shows that users are not bothered by permanently sharing their location with their friends, we believe that allowing one time requests may be more desirable. When a request is performed the user does not need to be immediately notified (and bothered by this fact), especially if he has authorized the requester to request about his location at any moment. However, the request is logged for future analysis.

V. Metrics for evaluating WLAN localization

Localization is defined as a mechanism to find spatial relationship between objects [19]. Fundamentally speaking, location systems require some kind of inputs - either connectivity information or signal strength/timing information received from the beacons. Regardless of what the source of this information is, it is then used as an input to the location techniques such as triangulation, proximity, or scene analysis to derive objects location (either absolute or relative location). A detailed survey on the techniques and technologies that are enabling both indoor and outdoor localization can be found in [20].

Depending on the required range, propagation speed, cost, precision, bandwidth, etc., one can choose the required technology for a specific application.

We have defined the following parameters, which can be used as guidelines to compare and evaluate several indoor location/positioning systems. More metrics for evaluating localization algorithm is addressed in [20].

1) *Accuracy and Precision* of estimated location are the key metrics for evaluating a localization technique. Accuracy is defined as, how much the estimated position deviates from the true position and is denoted by an accuracy value and precision value (e.g. 15 cm accuracy over 95% of the time). The precision indicates how often we expect to get at least the given accuracy. The accuracy of a positioning system is often used to determine whether the chosen system is applicable for a certain application.
2) *Calibration* is also very important. The uncalibrated ranging readings are always greater than the true distance and are highly erroneous due to transmit and receive delays [21]. Device calibration is the process of forcing a device to conform to a given input/output mapping. Often there is a tradeoff between the accuracy and the calibration effort.
3) *Scalability* is a significant parameter, as the proposed technique should be scalable for large networks. If an approach is calibration intensive then eventually it is not a scalable solution.
4) *Cost* is also a crucial issue. It includes the cost of installation, deployment, infrastructure and maintenance.
5) *Privacy* arises major concerns and should be definitely taken into account since its conception is important. Using localization it is very easy to create a Big Brother infrastructure that track users movements and allow to deduce patterns of behavior. However, this issue is being generally overlooked in the design of systems and considered as an afterthought only. Centralized systems are particularly weak with regard to privacy.

VI. Localization in FLAVOUR

A premise of our work is that signal strength information provides means of inferring user location. The IEEE 802.11 standard defines a mechanism by which RF energy is to be measured by the circuitry on a wireless NIC. In 802.11b/g/a, this numeric value is an integer with an allowable range of 0 – 255 called the Received Signal Strength Indicator (RSSI). 802.11 does not require that a chipset vendor use all 255 values, so each vendor will have a specific maximum value. For example, Cisco chooses RSSI-max as 100 while the atheros chipset use 60 as the maximum value. Thus, the *Spotter* will measure a signal strength value between 0 and 255 for each of the access points in the vicinity. The location of the access points in 3D coordinate system is maintained in a database, which in our case is part of the University's administration.

Table I shows an example of *scanning*. The scanning process outputs a list of the MAC addresses of access points associated with the signal strength observed in the scan (probe response frames).

TABLE I

An example of access point scanning

AP BSSID	SignalStrength	SSID
000b5fd00de8	-75	WLAN
000b5fbcc0e0	-91	WLAN
000b5fd7f214	-88	WLAN
000b5fd00d2e	-82	WLAN
000b5fd7f1c5	-45	WLAN
000b5fd7f1d6	-61	WLAN

Calibration consumes human labor and creates significant maintenance and scalability issues. Hence our objective is to present a calibration-free localization technique that eliminates the laborious offline RSSI measurements.

In this section, we first describe two existing calibration-free location techniques, namely, the *Cell of Origin (CoO)* technique and *Centroid (Cent.)* technique. Consequently, we propose a new calibration-free technique called *Enhanced Centroid (Enh. Cent.)* technique. Finally, we present an analysis of how well these techniques perform using our experimental data in section VII.

*A. **Cell of Origin technique***

It is a simple positioning algorithm, directly derived from the mobile phone positioning used in cellular networks. In WLAN network coverage is provided by a number of distributed access points. It is assumed that the user is located in the vicinity of the strongest heard access point or associated access point. The location coordinates of the access point whose signal strength is the strongest is retrieved from the access point database and is considered as the user's location. The disadvantage of this method is obvious since accuracy of the location estimation depends on the range covered by the access points (see table II).

*B. **Centroid technique***

In the scanning phase of the Centroid technique, all the readings that are received from the access points within the range are combined. The top three strongest heard access points are chosen and their coordinates are retrieved from the database. This information is used to position the user at the center of these access points. This simple technique, merely uses the access points having strongest signal strength and their coordinates to obtain the user location. However, as it is shown in Section VII-B, due to inherent variation in the signal strength at indoor environments this method is not reliable. The performance of the technique is reported in Table II.

C. ***Enhanced Centroid technique***

In the previous techniques, signal strength is merely used to filter out the access points. However, having a strong signal strength does not necessarily mean that the user is close to that access point. Taking into account the distance to the heard access points can greatly enhance the localization result. This is the basic idea behind our algorithm. Following the observation of [20] stating that any range-based localization algorithm works in three phases, i.e., ranging, distance approximation and refined location estimation, our technique will perform the following steps:

1. Scanning for AP: As a first step, the signal strength measurements are obtained from the scanning process as explained before.

2. Noise reduction: Signal strength measurements at indoor environments are not reliable since they are associated with both time-varying errors and environmental-dependent errors. Time varying errors mainly occur because of additive noise and interference and can be significantly reduced by averaging multiple measurements over time. Hence, we use an exponential moving-average filter to reduce the anomalities caused by the noise and smoothen the received signal strength. Equation 1 shows the formula. Environmental errors are the result of the physical arrangement of objects (buildings, trees and furniture) in a particular environment. Since environmental errors are unpredictable they are considered as a random variable. However in a particular environment objects are predominantly stationary. Thus, for a network of mostly stationary sensors, environment-dependent errors will be largely constant over time.

$$CurrentSS = \alpha * (1 - CurrentSS) + \alpha(PreviousSS) \tag{1}$$

Equation 1 states the current signal strength (CurrentSS) value is a linear aggregate of the previous signal strength (PreviousSS) value and an independent noise factor (α). The parameter α gives the flexibility to the model and can take any value between 0 and 1.

3. Sorting: Depending on the density of the access points in the test area, the number of heard access points varies. In order to make a short list of the candidate access points to be used by the location algorithm, they are sorted in descending order and the top three are chosen.

4. Location approximation: A rough estimation of the location is obtained by computing the distance between the mobile device and the top three chosen access points. The computed distance, is used to generate a new set of coordinates on the lines connecting the chosen access points.

5. Enhanced centroid: The set of newly obtained coordinates is taken as input to compute their centroid leading to a better location estimation.

6. Refinement: Due to the variation in signal strength, the estimated location fluctuates quite often even at static places. In order to reduce this fluctuation, we use a time averaging technique to refine the accuracy of the final location estimation.

VII. Experimental evaluation

A. *Test bed set up*

We performed our experiments in the fourth floor of the Zilverling building of the University of Twente. Figure 4 shows the layout of the floor. The test bed has a dimension of 106 m by 14.5 m. It includes a long hallway and many rooms. The floor contains four access points that are mounted on the ceiling and are placed in a straight line. They operate in 2.4 GHz band. The transmission power of the access points is 50 mW. To study the signal propagation and perform measurements, we used a HP Compaq nc6000 laptop with built-in WLAN card. We used the *Spotter* to capture the RSSI from each access point. All coordinates are measured in the RDNAP coordinate system.

B. *WLAN signal analysis*

To analyze the behaviour of the signal strength in the test bed, we measured the signal strength from a single access point over a period of 2 minutes. We took 120 samples at 1 second intervals. Figure 5 shows the variation of signal strength from one access point. Variations can be seen as large as 8 - 10dBm in the measured RSSI. The reason for this variation is mainly because the signal measurements are associated with errors. In the same figure, the smoothened signal values using Equation 1 for different values of α are plotted. One can observe that the higher the value of α, the lesser the smoothening effect. However, there is a tradeoff between the smoothening versus the time required for

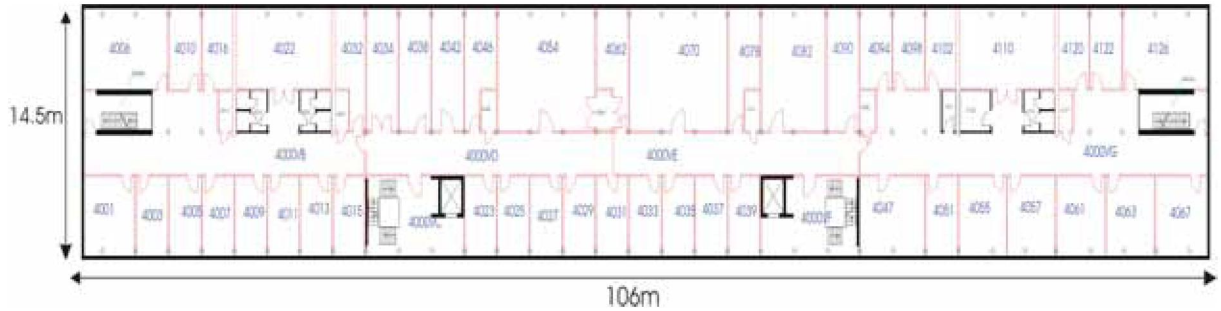


Fig. 4. Floor plan of the building where the measurements are performed

smoothening. As it is shown in Figure 5, we found $\alpha = 0.2$ as an optimal value.

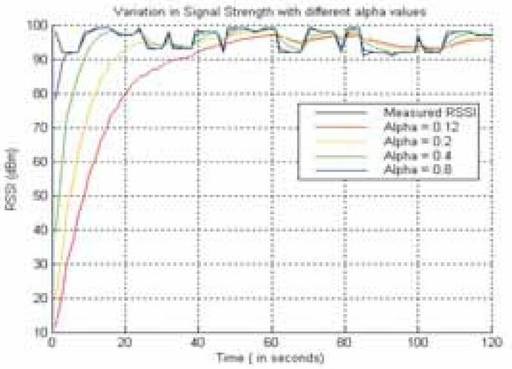


Fig. 5. Variation in signal strength and effect of smoothening

C. Results and Discussions

In this section, the performance of the three mentioned localization techniques is evaluated by computing the median accuracy. The Centroid technique achieves median accuracy of 1.8 - 18m (horizontal accuracy) and estimates the correct floor 60% of the measured time (25 minutes) while our proposed technique, which incorporates the smoothing and refining phase, yields median accuracy of 0.45 - 8m and estimates correct floor 75% of the measured time (25 minutes). Table II summarizes the results of our measurements. Since we have not performed experiments on the CoO technique, we cannot report its vertical accuracy.

Localization accuracy depends on many factors such as calibration, placement of the access points, access point density, environmental factors, etc., During our measurement we observed that, when the required number of access points falls below the minimal requirement as specified in table II, the performance is bad and the localization error can go up to 10m to 15m. Also, the fact that all access points used in these tests lie on a straight line, makes the estimate less accurate. When the measurements are done right under the access point, the horizontal accuracy is less than 0.2m, but the floor is determined correctly only 50 percent of the time. This is because the access points in our multi-storeyed building are situated right below each other, leading to situations in which sometimes the access points in the floor below will have same X,Y position and give a strong signal, which is used in the calculation. A general remark is that, when the access points are in triangles instead of being in a straight line (as we have), the accuracy can be determined even better using the enhanced centroid algorithm. Since the WLAN localization is performed as an add-on to the existing infrastructure, the access points are deployed in such a way that they give best coverage. However, placing the access points in a more optimal way, can result in a much better location accuracy.

TABLE II
COMPARISON OF CALIBRATION-FREE WLAN LOCALIZATION ALGORITHMS.

Method-Feature	**CoO**	**Cent.**	**Enh. Cent**
Minimum AP	1	3	3
Horizontal accuracy	10-25m	1.8-18m	0.45-8m
Vertical accuracy	NA	60%	75%

In order to reduce the effect of errors caused by the environment, we are planning to develop a model-based algorithm which uses the geometrical properties of the buildings.

VIII. CONCLUSIONS AND FUTURE WORK

An early prototype of FLAVOUR was demonstrated at the SVGOpen conference held at UT [22]. That version of FLAVOUR did not have the *Lookup service*, the *FLAVOUR server* was not distributed and the localization algorithms used were in an earlier development stage. At the end of the conference attendees filled in a short conference survey that, among other questions, included the following: If you participated in the FLAVOUR experiment, were the offered services useful and easy to use?" The majority of the surveyed participants provided a positive feedback. The main suggestion by a large group of participants was to improve the location accuracy. Few complained about difficulties using some of the services, like locating friends, as at that time there was no service to choose and select other participants' services. The participants had to know their friends identifiers in the system, and provide FLAVOUR with that identifier to get access to the services.

The prototype tested was only available for laptops and many participants were not happy with that restriction. They suggested that PDAs should be more useful. At present we are working on making the software available on PDAs. Another useful suggestion was to include some sort of profiling at the time of registering in FLAVOUR, to ease the job of searching for people and adding contacts.

Regarding localization, on-going work includes enhancing FLAVOUR by developing yet better localization algorithms, and incorporating Spotters for handling other type of hardware and technologies. For example, we are already working in localization techniques using Wireless Sensor Networks (WSN).

Regarding the FLAVOUR architecture we are going to add more intelligence to the *Privacy Guardian* by incorporating agents that can use context-aware information. We believe that the architecture of FLAVOUR can be easily extended to provide more services, as for example sharing sensed data or context-aware information. At present we are researching those possibilities.

Acknowledgements

This work is part of the *Smart Surroundings* project, funded by the Ministry of Economic Affairs of the Netherlands under the contract no. 03060.

Authors would like to thank Department of Information Technology, Library & Education (ITBE) of University of Twente and Drs. Barend Köbben from ITC, respectively, for manual mapping of the access points and providing enormous help in respect to geo-database.

References

[1] "http://www.newscientist.com/article.ns?id=dn3834."

[2] M. Langheinrich, "Privacy by design - principles of privacy-aware ubiquitous systems," in *Proceedings of Ubicomp 2001*, Atlanta, GA., 2001.

[3] M. Langheinrich and S. Lahlou, "Troubadour approach to privacy," Ambient Agoras, Tech. Rep. Disappearing Computer Initiative 15.3.1, Nov. 2003.

[4] A. F. Westin, *Privacy and Freedom*. New York NY: Atheneum, 1967.

[5] "Spot me." [Online]. Available: http://www.spotme.com/

[6] D. Cox, V. Kindratenko, and D. Pointer, "Intellibadge," in *Procs of 1st International Workshop on Ubiquitous Systems for Supporting Social Interaction and Face-to-Face Communication in Public Spaces, 5th Annual Conference on Ubiquitous Computing - UbiComp 2003*, 2003.

[7] Borovoy.R, Martin.F, Vemuri.S, Resnick.M, Silverman.B, and Hancock.C, "Memetags and community mirrors:moving from conferences and collaboration," in *Proceedings of ACM conference on Computet Supported Cooperative Work*, 1998.

[8] "Charm badge." [Online]. Available: www.charmed.com

[9] "ntag interactive." [Online]. Available: www.ntag.com

[10] P.Bahl and V.Padmanabhan, "RADAR: An inbuilding RF based user location and tracking system," in *IEEE Infocom*, vol. 2, March 2000, pp. 775–784.

[11] P.Castro, P.Chiu, T.Kremenek, and R.Muntz, "A probabilistic room location service for wireless networked environments," in *Proceedings of Ubiquitous computing*, 2001.

[12] J.Small, A.Smailagic, and D.P.Siewiorek, "Determining user location for context aware computing through the use of wireless lan infrastructure."

[13] M. Youssef, A. Agrawala, and U. Shankar, "Wlan location determination via clustering and probability distributions," in *Proceedings of IEEE PerCom 2003 (PerCom03)*, march-2003.

[14] A. M.Ladd, K. E.Bekris, A. Rudys, G. Marceau, L. E.Kavraki, and D. S. Wallach, "Robotics based location sensing using wireless ethernet," in *Proceedings of the Eigth ACM International Conference on Mobile Computing and Networking (MOBICOM)*.

[15] "Ekahau positioning system." [Online]. Available: www.ekahau.com

[16] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, J. Tabert, P. Powledge, G. Borriello, and B. Schilit., "Place lab: Device positioning using radio beacons in the wild," in *Proceedings of Pervasive'05*, May 2005.

[17] W. G. Griswold, P. Shanahan, S. W. Brown, R. Boyer, M. Ratto, R. B. Shapiro, and T. M. Truong, "Activecampus: Experiments in community-oriented ubiquitous computing," *IEEComputerM*, vol. 37, no. 10, pp. 73–81, Oct. 2004.

[18] S. Lederer, A. K. Dey, and J. Mankoff, "Everyday privacy in ubiquitous computing environments."

[19] N. Bulusu, "Self-configuring location systems," Ph.D. dissertation, University of California, Los Angeles, 2002.

[20] K. Muthukrishnan, M. Lijding, and P. Havinga, "Towards smart surroundings: Enabling techniques and technologies for localization," in *Proceedings of the International Workshop on location and context awareness (Loca2005)*, 2005.

[21] K. Whitehouse, "The Design of Calamari: an Ad-hoc Localization System for Sensor Networks," Master's thesis, University of California at Berkeley, 2002.

[22] K. Muthukrishnan, N. Meratnia, M. Lijding, G. Koprinkov, and P. Havinga, "Demonstrating flavour: Friendly location-aware conference assistant with privacy observant architecture," in *Proceedings of the third international conference on Service oriented Computing(to be publised as Technical Report)*, 2005.