Research Article

A Scalable and Privacy-Aware Location-Sensing Model for Ephemeral Social Network Service

Yongqiang Lyu,1 Dezhi Hong,1 Ying Wang,1 Yinhong Hou,1 Zhengwen Yang,1 Yu Chen,1 Yuanchun Shi,1 and Alvin Chin2

1 Research Institute of Information Technology, Tsinghua University, Beijing 100084, China
2 Nokia, Dong Huan Zhong Lu, Daxing, Beijing 100176, China

Correspondence should be addressed to Yongqiang Lyu; luyq@tsinghua.edu.cn

Received 10 November 2012; Revised 1 February 2013; Accepted 17 February 2013

Copyright © 2013 Yongqiang Lyu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Social network services (SNSs) are developing at an explosive speed, which makes it easy for people to be closely connected. As a result, a new SNS type, ephemeral social network (ESN), is emerging to capture the ephemeral interactions and meetings that occur in environments such as conferences and workplaces. Most ESNs require the positioning for capturing the physical proximity between people, which impacts much the scalability, privacy protection, and the cost of the system. In this paper, we propose a scalable location-sensing model based on RFID-sensing architecture for ESN in consideration of four aspects of requirements, that is, the usability, QoS, scalability, and privacy. The model includes the perspectives of the privacy, architecture, deployment, and positioning algorithms, which can meet the four key requirements. A prototyping conference-type ESN system was also developed in this paper and was tested in the ACM UbiComp 2011 conference, which verified that the model works well with good scalability, low cost, and customized privacy protection.

1. Introduction

Social network services (SNSs) have become ubiquitous and been developing at an unprecedented speed to connect people with each other. The use of SNS also appears in many specific ephemeral scenarios and occasions, like academic conferences and workplaces, which is known as the ephemeral social network service (ESN) and gradually show its necessity. ESNs could provide each user with the location of peer users and their activities based on locations. As many other indoor ubiquitous applications, the positioning (location-sensing) system becomes the key component to obtain position-related information of an ESN since most ESNs are position-sensitive applications and are mostly used indoors, where global positioning system (GPS) or assisted GPS (AGPS) fails to work effectively and accurately.

When choosing techniques to fulfill the requirements of the location-sensing system for an ESN, we should take into account the following four perspectives of requirements as Figure 1 shows.

(i) Usability. This part involves the operability, flexibility, cost, and convenience in terms of system deployment, configuration, and use. These issues must be evaluated: how the operability of the system is, whether it is complex to set up or make adjustments, whether the system has any special requirements on the devices, what the cost is, and whether the users need to wear extra specific apparatus or devices. Usability of the system determines how much it could be accepted by users.

(ii) Quality of Service (QoS). This part consists of two aspects, that is, the power consumption and positioning accuracy. The power consumption is a key issue because ESNs would be utilized mostly in mobile scenarios, such as on mobile phones, PADs, and wearable sensors, all of which have limited battery capacities. Therefore, the power consumption of the location-sensing system must be controlled within
the accepted level. As for the accuracy, the location-sensing system should achieve certain resolutions according to the application requirements: in some cases it may be in the order of meters, while in some other cases it may be in the order of centimeters; it could be tuned automatically or manually by users according to different demands of using scenarios, for example, due to privacy policies.

(iii) Scalability. Most positioning technologies could be working well when supporting tens of users. However, when the amount of the users becomes larger, for example, hundreds or more, some kinds of techniques would fail to meet the requirement of scalability, for example, degrading in performance, usability, QoS, and so forth.

(iv) Privacy. Since a positioning system could achieve certain accuracy of the user’s location information, the user’s locations might be exposed and the system should involve the policy of a controllable privacy hierarchy from the perspectives of the user security levels, location-sensitive area types, and the activity-based accuracy requirements. All these are differently configured for each user because it contains users serving different roles of initiator, common user, evaluator, and analyst [1] for a specific ESNS; it covers effective areas providing services of different activities and holds several kinds of activities that can cause variation in using the same area. We should combine these concerns to standardize our model to meet the requirements of each privacy hierarchy, respectively.

In this paper, we firstly make comparisons among several state-of-the-art location-sensing technologies with respect to the four aspects of requirements and then present a scalable and privacy-aware location-sensing model dedicated for the ESNS under several typical scenarios. The reminder of the paper is organized as follows. Section 2 gives a comparative overview of the current positioning technologies and some related work that has been undertaken. Section 3 discusses the privacy issues for a standard ESNS and the corresponding privacy-aware and scalable model is shown in Section 4. In Section 5, the ESNS system we developed, the Find & Connect UbiComp at the UbiComp 2011 conference, is shown as an experimental verification to our location-sensing model.

2. Related Work

Many technologies are currently utilized to provide indoor positioning services such as image, infrared, Wi-Fi, RFID, and UWB. In this section, we make a discussion on the advantages and disadvantages of them to the four requirements respectively as listed in what follows.

2.1. Unobtrusive Methods. The positioning methods, such as image-based [2], infrared [3], ultrasonic [4], and inertial methods [5], do not need any additional accessories worn on the users and thus are classified as unobtrusive methods in this paper. Recently, Microsoft Kinect [6, 7] becomes another option for indoor positioning by exploiting the image depth. However, the common disadvantages [8] of these methods are: (1) inaccurate positioning results, (2) inability to sense subjects due to the blockages of the walls, ceilings, and so forth, and (3) weak scalability to the large user volume due to the cost and the difficulty in user recognition.

2.2. ISM Radio-Frequency Methods. The industrial, scientific, and medical (ISM) bandwidths are reserved for daily communications in many countries and regions, for example, the Bluetooth, Wi-Fi, ZigBee, and RFID of 2.4 GHZ. These communication methods can also be employed in indoor positioning by utilizing the radio signal strength (RSS), such as Wi-Fi positioning [9], RFID positioning [10], and ZigBee positioning [11]. The most obvious advantage of using ISM communication methods is that such kind of system could share the same infrastructure as that of existing indoor wireless networks and needs little pre-setup. However, the long-term access to the ISM networks (such as Wi-Fi access points) by mobile devices or user tags may be power-consuming and requires extra ability of wireless access on user devices. The accuracy of such positioning systems is also relatively low. In addition, the costs of some communication chips are often high due to the intellectual properties (IPs) of the protocol stacks, such as Wi-Fi and Zigbee.

2.3. Wideband Radio-Frequency Methods. Ultra wideband (UWB) [12, 13] positioning utilizes the advantage of the wide band of the communication and can achieve high positioning accuracy with the error of couple centimeters [14]. However the chip of UWB is expensive and the power consumption is also high. Recently, there is another alternate method named chirp spread spectrum (CSS), which operates in narrower bandwidth than UWB but can achieve comparable positioning accuracy and ultra low power [15]. Both UWB and CSS positioning can employ time of arrival (TOA), time difference of arrival (TDoA), and radio signal strength (RSS) to sense the locations and TOA/TDoA can be more accurate than RSS. Nevertheless, the cost and power issues of UWB and CSS are still the key factors determining the usability.

2.4. Active RFID. In comparison with other related technologies, the active RFID positioning systems can gain the following advantages over the others.

Usability. With regularly distributed RFID readers collecting active tag signals, a central server is enough to process the
data and calculate the location for hundreds of tags. The system architecture is therefore simple and easy to deploy and maintain.

Although the cost of a RFID reader is relatively a little higher than a Wi-Fi access point (AP), we can regard the installation of the RFID readers as infrastructure and they can actually cover much wider area than Wi-Fi APs (up to 150-meter radius), which means we do not need to set up so many readers for the same coverage as other positioning methods especially in the scenarios of low resolution. Another important advantage of RFID is that the RFID tags are cheap (e.g., cheaper than Wi-Fi) and also easy to wear. When deploying ESNS in, for example, the academic conferences, the organizers only need to distribute the RFID tags to attendees and retrieve the tags after the activity, which provides much convenience and efficiency to both the organizers and users.

**Quality of Service.** For power consumption, an active RFID tag with a normal battery can theoretically last for 3–5 years at the medium data rate under the current technology node; while the Wi-Fi tags or phones suffer the remarkable power consumption which degrades the QoS. As for the accuracy, active RFID systems can reach high accuracy using algorithms with proper distribution of readers and reference tags (can be higher than Wi-Fi) and can be adjusted to lower resolutions using simple algorithms with fewer readers.

**Scalability.** A single RFID reader supports flexible user volume, ranging from dozens to hundreds, which is enough to cover most ephemeral social scenarios. The positioning system made up of several RFID readers could support up to 1k users simultaneously with only average computing resources.

**Privacy.** The resolution of location information provided should be controlled with respect to privacy requirements from users. The strict privacy policies should be set to sensitive scenarios by default, such as rest rooms, dressing rooms, and smoking area, and the RFID-based accuracy-adaptive algorithms and deployment can also meet this requirement easily with low cost.

In summary, a RFID-based positioning system is suitable for a scalable, low-cost, QoS-controllable and privacy-protecting ESNS. The practical model is described as follows.

### 3. Privacy

#### 3.1. Location Privacy in ESNS

According to Duckham and Kulik [16], the concept of location privacy can be generally defined as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.

It suggests subtle preferences of revealing location data in different forms for common positioning services [17].

(i) **When.** A subject may be more concerned about his current or future location being revealed than locations from the past.

(ii) **How.** A user may be comfortable if friends can manually request his location but may not want alerts sent automatically whenever he enters a toilet or a bar.

(iii) **Extent.** A user, in some cases, may rather have his location reported as an ambiguous region rather than a precise point.

As for indoor positioning, especially for ephemeral social network service, we should consolidate the guidelines above as follows.

(i) **When.** As ESNS explores possibility to know people in physical proximity where each encounter happens and lasts at random, users may be more concerned about their past and current location as well as those of others in certain connection with themselves, which should be provided by the system with a possible form of recommendation pushing.

(ii) **How.** The users should have sufficient controllability over their own position data in the sense that (1) they can view and edit private location records, and (2) they can manually decide whom to share the location data with and how much information to reveal. There should also be data-mining recommendation algorithms based on physical proximity and social connections in the system to automatically raise attention among those people who should have been connected but not yet connected in real life.

(iii) **Extent.** The users may still want their locations reported as ambiguous regions rather than precise points in most public places. However, in specific areas holding social gatherings such as parties and conferences, the participants would raise their tolerance for location privacy but care more about knowing people with a clear overview of “who and where” in the room. Therefore, as for an ESNS, such areas require higher accuracy in positioning, while other public places such as passageways and rest rooms need only ambiguous or even no position reports.

With the concept of location privacy refined for ESNS applications, now we can explore more about the location and privacy issues in the following section.

#### 3.2. Privacy Concerns from the User

In previous studies, researchers have found that most users do not care about their location privacy as much as what the computer scientists have designed and advocated. According to a study of 55 interviews with subjects in Finland, Kaasinen [18] found that “The interviewees were not worried about privacy issues with location-aware services.” However, he added, “It did not occur to most of the interviewees that they could be located while using the service.” In another study of university students, Danezis et al. [19] asked 74 undergraduates how much they
would have to be paid to share a month’s worth of their location data. The median price was £10, or £20 if the data were to be used commercially. For most indoor positioning services, navigation combined with preference information pushing is a common purpose. Users are willing to reveal their location information to the system with the attention focusing on the services, and the services they expect to get from the system often ignore the possibility of location leak to unauthorized attackers.

Nevertheless, the privacy concern is more severe in the case of ESNS. Judging from the feedback from our own system Find & Connect UbiComp, a conference-based ESNS, some of the users had serious concerns about how the organizers would deal with all the location data. So the privacy concerns arise again under the ESNS circumstances such as the conference, where users have direct knowledge that their locations may be seen by others after permission, and some private information such as with whom they stay in proximity could be revealed. Therefore, we emphasize on “how” we should carefully define user activities in ESNS, as discussed in the previous parts, to protect privacy and compromise positioning accuracy to a reasonable extent.

3.3. Service Requirements. From the discussion above, the model of indoor positioning services in ESNS requires the following basic functions:

3.3.1. Security Access Levels. Considering the different statuses of the users, they have accordingly different levels of access to the position information of the targets. For common users, they can only access the locations of those who willingly share their information; as for authorized guardians like system administrators, they can have higher control over tracking and monitoring the targets. But their free access to all the data might also raise privacy and security issues and we will further discuss it in Section 4.

3.3.2. Controllability over Personal Data. Common users should personally decide whether to share their location information with people at the same or lower security access levels but would stick to the supervision from the higher levels to a legal extent. As for those controllable information, they can also treat different people in different ways, namely, they can specifically choose whom to share the information with.

3.3.3. Availability in History Records. Both for the system administrators to monitor and maintain the system and for common users to retrospect on places they have been to, it should be available for them to access the history data. Nevertheless, it is also constrained with respect to their security access levels.

3.3.4. Accuracy Variation for Specific Areas. Privacy limits the accuracy of the indoor positioning due to various functional zones/area in a given ephemeral social network space. On the one hand, for the highly gathering places where the social activities take place, the accuracy of location sensing could be high because users normally care more about the social activities in the willingness to be connected with other people in the same event; the position information is regarded open and ready to be achieved by others. The possible threats of position information leak are not the issues. On the other hand, for the public places which are more privacy-sensitive, such as dressing rooms, rest rooms, and smoking places, the participants may need personal activities, the positioning accuracy should be lowered or obscured to protect user’s privacy.

4. Location-Sensing Model

In this section, we firstly introduce the general architecture and the functions of each part of this model. Then we present the deployment model that could be utilized in general cases. In the following parts, we describe the details of the positioning algorithms and the privacy control, respectively.

4.1. Architecture. As Figure 2 shows, the architecture of the model from top to bottom is the application layer, information-processing layer, and physical-collection layer. The relationships between the adjacent layers and the respective content are described in Figure 2.

4.1.1. Application Layer. The application layer is the top-most layer which handles the ubiquitous ESNS services provided to users. Some features and services in this layer depend on the position-related information and the data provided by the adjacent lower layer through stipulated interfaces. In the implementation of this paper, the Find & Connect application is realized in this level based on the interfaces of the information-processing layer. For some extended applications, the developing application programming interfaces.
(APIs) can also be built in this layer to support more applications.

4.1.2. Information-Processing Layer. This intermediate layer implements certain algorithms to process and analyze the raw data transported from the physical layer and extracts necessary characters and information provided to the upper application layer. For example, the filtering algorithms can be placed in this layer to support the subject-tracking services in the application layer. Some filtering algorithms may need intensive data support from the databases, and the databases are thus also classified into this layer.

4.1.3. Physical-Collection Layer. This layer contains all the sensors and devices used in the positioning system; it handles the deployment as well as the configuration of the hardware systems. Physical-collection layer directly collects signals and related data transmitted from the devices, such as from the tags, which are processed in the upper information-processing layer. Some communication middleware and protocols are often needed in this layer to parse the physical signals from the sensors and devices into data format.

4.2. Deployment Model. We have two deployment schemes to meet the requirements of positioning accuracy, that is, the high-accuracy scheme and the low-accuracy scheme.

4.2.1. High-Accuracy Scheme. In average ESNS scenarios such as academic conferences, office buildings and public areas, the requirement of high positioning accuracy is just in the level of around one meter; the resolution of centimeter-order which can be achieved by UWB is often not necessary. LANDMARC [10] is a widely used active RFID-based positioning algorithm, which has low deployment complexity and stable performance. Therefore we adopt the positioning algorithm based on LANDMARC [10] and a hardware system consists of RFID readers and a certain number of reference tags. The LANDMARC algorithm is based on the idea that the user-tag location could be calculated by employing the known locations of the reference tags in the same space. This algorithm was also verified working well with reasonable accuracy in our experiments.

The general placement scheme of the RFID readers and reference tags is the core issue of the entire deployment model, and we propose a general scheme for it which can be employed in most common scenarios. We set 4 anchoring RFID readers with omni directional antennas in the target space with their distributive positions meeting the following requirements: (1) all four readers head towards the center of the room; (2) the four readers' positions form a rectangle-like quadrilateral; (3) the quadrilateral covers the target space to the greatest extent; and (4) each reader should minimize the blockage in its way of signal collection. We also set several assistive readers placed at the midpoint of the two longest edges of the rectangle formed by the four anchoring standard readers, as the example in Figure 3(a) shows, which can help improve the coverage of the radio frequencies in large space or places with blockages. Particularly, when the amount of the tags detected by any of the assistive readers surpasses any of the anchoring ones, the assistive reader should take over the anchoring reader to work and collect the data for positioning. Figure 3(b) shows other two placement examples to illustrate the deployment scheme for different target space shapes (vertical view).

Particularly in cases of irregular target spaces, the regular placement of the readers is recommended in this paper because the regular placement can lower down the complexity and improve the stability of the positioning algorithms. However, the interior placement, for example, the Case B in Figure 3 for the irregular space, often leaves some uncovered space outside the rectangular coverage of the readers, which may lower down the positioning accuracy within this area.

4.2.2. Low Accuracy Requirement. For low-accuracy requirements, such as the room-resolution level in which the users can only be recognized if they are in the room, we can employ the coarsening deployment model including the radio signal strength (RSS) justification scheme and the IP address-stamping scheme.

RSS Justification. The positions of the readers in each room should meet the following conditions: (1) setting readers according to the whole area or divided sections of the room; normally one reader for one room; (2) placing the reader of a room on the side far from the gate and the passageway to minimize the interference between the signals of adjacent rooms; (3) maximizing the signal range of the reader to cover as much as possible inside the room but as little as possible outside the room. With the deployment scheme, a specific RSS threshold for the reader of the room achieved from the
manual training or machine learning can be adopted to justify whether a user is inside or outside of the room.

Given any two adjacent rooms, in the signal-overlapping areas of the two contiguous readers of them (in the case of one reader for one room), the RSS values of a user-tag to each reader can be compared to decide which room the tag belongs to especially when there is a wall between them which can often dramatically lower down the RSS values of the signal-through reader. The method is statistically verified efficient in this paper.

IP Address Stamping. Radio signals transmit in its constant speed; a reader can have its unique address of either IPV4 or IPV6 in a given networking configuration. Whenever the signal of a user-tag is collected via the IP-stamped reader, the backend signal-processing server can justify which reader it is from. If there are two closely adjacent signals analyzed at the server, the earlier-coming one will be preferred to be valid and the location of the reader will be regarded as the tag position in the low-accuracy scenario.

4.3. Algorithms. According to the deployment model above, we have different algorithms for each deployment scheme. See Figure 4.

4.3.1. High-Accuracy Scenario. In scenarios which require high sensing accuracy, the positioning system of this paper just employs the LANDMARC algorithm, which is proposed by Ni et al. [10] and was verified in the tests of this paper. LANDMARC works with the idea that the unknown positions of the active user tags could be calculated with the already-known fixed positions of reference tags since they are all placed in the same space.

Assume we have n RFID readers, m reference tags, and N user tags to track, respectively, n is set to 4 in the model of this paper, and we get the signal strength vector (SSV) of a user tag $p_i, i \in [1, N]$ as

$$S_i = (S_{i1}, S_{i2}, S_{i3}, S_{i4}),$$

where $S_i$ denotes the signal strength of the user tag $p_i$ received by reader 1 to 4.

For a reference tag $r_j, j \in [1, m]$, we have similar signal strength vector as

$$\theta_j = (\theta_{j1}, \theta_{j2}, \theta_{j3}, \theta_{j4}),$$

where $\theta_j$ denotes the signal strength of the reference tag $r_j$. Then we can calculate the Euclidean distances $E_{ij}$ from the user tag $p_i$ to an arbitrary reference tag $r_j$ with respect to the SSVs of them:

$$E_{ij} = \sqrt{\sum_{n=1}^{4} (S_{in} - \theta_{jn})^2},$$

where $i \in [1, N]$ and $j \in [1, m]$. The nearer the user tag to track is to the reference tag, the smaller the Euclidean distance $E$ between them will be.

Then the distance vector for each tag $p_i$ can be obtained as $E_i$ with respect to $m$ reference tags:

$$E_i = (E_{i1}, E_{i2}, \ldots, E_{im}).$$

For each tag $p_i$, we selected 4 reference tags with the smallest $E$ values as calculation basis, and then the respective weight $w_{ij}$ between $p_i$ and $r_j (j \in [1, 4])$ can be calculated

$$w_{ij} = \frac{E_{ij}^2}{\sum_{j=1}^{4} E_{ij}^2}.$$

From the LANDMARC algorithm, the position of the user tag $p_i$ can be then calculated as

$$(x_i, y_i) = \sum_{j=1}^{4} w_{ij} \times (x_j, y_j),$$

where $(x_j, y_j)$ is the coordinate of user tag to be evaluated and $(x_j, y_j)$ is the coordinate of one of the 4 selected reference tags. The position of user tags can thus be calculated with relatively high accuracy.

4.3.2. Low-Accuracy Scenario. In scenarios with low-accuracy requirements, we employ corresponding low-accuracy algorithms to fulfill the positioning. There are two algorithms in this category.

Hybrid Zoning Algorithm. We employ a combined zoning and RSS-justification algorithm. The transmitting power of each reader is preset to adjust the signal-detection capacity and make it cover the zone of a certain area which is preconfigured in deployment. In order to avoid any blind point in each zone, two contiguous zones would have some overlaps. We define $S_{kj}$ as the signal strength of tag $k$ received by reader $j$, whose coverage zone $j$ has an RSS threshold $S_j$. We configure the reader to make sure that all $S_{kj}$ of tags inside the zone $j$ will satisfy $S_{kj} \geq S_j$, and satisfy $S_{kj} < S_j$ when they get outside of the zone $j$. $S_{kj}$ is obtained from testing or training before deployment, which is a relatively stable value monotone with respect to the radius of the zone. For the overlapping zone of the two contiguous zones $i$ and $j$, tag $k$ might satisfy $S_{kj} \geq S_j$.
\(S_i \text{ and } S_{kj} \geq S_j\) simultaneously. In this case, the position could be determined by comparing \(S_{kj}\) and \(S_i\); the tag is justified to be within the zone \(i\) if \(S_{kj}\) is larger. When making such a decision, we make a reasonable assumption that each divided zone covers almost a same area. If the areas vary a lot from one to another, the corresponding fencing schemes should be considered, which figures out each zone by the corresponding RSS thresholds \(S_i\). The context of the user tag would be employed to break the tie in the overlapping zones of two adjacent spaces.

**IP Stamping.** We also employ IP stamping scheme to add location information into the data frames returned from each reader. Since the RFID readers can work with IP protocols by connecting to a LAN or a WAN, different IP addresses can be set to reflect different locations. The data frame transmitted can be defined in XML format as shown in Algorithm 1.

When receiving a data frame, the server can obtain the position of tag \(k\) by extracting tag ID and IP information from the data frame. Then the location of a certain tag could be interpreted with the tag ID and its corresponding source IP. For two very-close frames from different IPs, the earlier-coming one will be preferred to be valid since it implies that the tag may be closer to the reader of the first IP than the second due to the constant transmitting speed of the signal. Such a method can simplify the work needed for low accuracy requirement positioning.

4.4. Privacy Control. Based on the analysis of the system requirements of the privacy control, this paper employs the methodology for the privacy control as follows.

(i) Role control for users: two roles should be distinguished: administrator and common user. Administrators can access the global configurations of the system and the common users can access only their personal data. No application entries are suggested for the administrators to see all the privacy data of the common users unless they select “yes” in the corresponding options. Nevertheless, all the privacy data are tracked by the system in the backend and can be used in offline scenarios after legal authorization achieved.

(ii) Privacy policy and configuration for common users: the privacy policy is displayed by default at the first-time start-up of the application, and it can be accessed whenever the user would like to via the user interface. There are also the privacy configuration options for the common users to setup, such as which information can be shared, whom the information can be shared to, when to share and where to share.

(iii) Support for adaptable positioning accuracies: the system is not required always to offer the same-level accuracy for each scenario in ESNS. For example, in the public areas, the positioning accuracy can be the highest, while in the private areas such as rest rooms, the accuracy should be coarsened. This paper suggests that the privacy should be also guaranteed in the physical-collection layer rather than only in the software.

5. Implementation and Results

We implemented an ESNS application for the academic conference scenario—Find & Connect [20], as a validation for our model, which was actually employed in the ACM UbiComp 2011 conference. In this section we (1) describe the system setup and configuration and (2) present the outcomes and data from the system we used.

5.1. System Deployment and Setup. The physical layer of the Find & Connect UbiComp 2011 system consisted of two parts: (1) the RFID readers whose coverage ranges were controllable and were able to reach as far as 50 meters; (2) the active RFID tags which the attendees needed to wear.

The core of the system deployment and configuration was the placement of RFID readers in the selected venues. There were two types of venues in UbiComp 2011, that is, the small classrooms sized about 6 m × 8 m where the tutorials and workshops were held, and the large rooms sized about 30 × 20 m where the main conference sessions were held. We deployed the location-sensing model according to the requirements of the different scenarios.

In small venues, the organizers did not need to implement a positioning system with high accuracy because of (1) the low QoS expectation from the attendees, (2) the small space, and (3) the cost issue. Actually the real need in this conference was just to know in which room the users were located in the tutorials and workshops. So the zoning algorithm was selected to process the RFID signals. The actual deployment of the RFID readers is illustrated in Figure 5.

However, in the large venue where the main sessions took place, the attendees would ask questions, would see what was happening, and would setup connections with adjacent seats. So the high-accuracy algorithm was required in the scenario. As shown in Figure 6, the large venue with irregular shape can also be covered by the deployment model of this paper. The four readers were placed to form a rectangle which can cover most of the seats in the venue.

There were 400+ attendees in the ACM UbiComp 2011 conference. Due to the large tag amount and the limited processing capacity of the RFID readers, the refreshing interval of each RFID reader was set to 6 seconds, which can guarantee processing all the requests while keeping the response time fast enough. The LANDMARC algorithm was used to give the location information of the user tags with the support of reference tags in this scenario.

In order to figure out how the amount of the reference tags can impact the positioning accuracy, the experiments with different number of reference tags in the large venue were done. The accuracy was evaluated as the relative error to the real coordinates in the room:

\[
\text{accuracy} = 1 - \frac{\sum_{i=1}^{N} \sqrt{(x_i - x_{i0})^2 + (y_i - y_{i0})^2}}{\sum_{i=1}^{N} \sqrt{x_{i0}^2 + y_{i0}^2}},
\]  

(7)
where \( N \) is the tag amount, \((x_i, y_i)\) is the calculated coordinates of a user tag, and \((x_{i0}, y_{i0})\) is the real coordinates of it. Figure 7 gives the testing results. It shows that the accuracy improved a lot with the amount of reference tags increasing when the amount was still little. But the system accuracy will begin to be stable after the amount of the reference tags was approaching 20 (after 15). That was also the main reason why we finally employed 14 reference tags in the implementation. The reference tags were placed evenly as Figure 6 shows to help improve the positioning accuracy of the target space.

5.2. Results and Conclusions. In this section, the corresponding results from the Find & Connect UbiComp 2011 are shown and analyzed.

5.2.1. User Configuration for Privacy. In the Find & Connect UbiComp 2011 system, the location information of each user was optionally exposed to other users and the option could be easily configured by the user via the graphic interfaces shown in Figure 8, where the privacy policy can also be published for users to review.

If the user checked the checkbox of Share Location, the real-time positions of the user could be seen by any user of the system. It was a global configuration. In personal configuration, more privacy rules could be adopted, such as sharing to specific friends, the shared regions, and the level of the positioning accuracy. All the privacy configurations were implemented based on the privacy model supported by the RFID sensing model of this paper.
5.2.2. Low-Accuracy Model. In small venues, the zoning algorithm was employed to give the user locations. In order to verify its accuracy, the testing both before and on the conference days was performed. The results can be seen in Table 1.

The data in rows 1 and 2 are the pretrial data before the conference days, in which we kept the tags A and B in a selected room statically for more than two hours and compared the collected coordinates with the actual positions; the results showed the error rates of 0.55% and 0.63%, respectively. And in rows 3, 4, and 5, the data are the results obtained from the tags of three tutorial speakers on the conference days, who gave their speech in a specific room during a whole day. We compared their calculated positions from the algorithm with the actual positions recorded manually and found out the results. The error rates of 0.74%, 0.60%, and 0.58% showed that the model of this paper could work stably even with attendees filled up in the room; especially in the real conference days, the amount of the users in each small classroom was about 40, which nearly reached the upper limit of the space.

5.2.3. High-Accuracy Model. In the large venue where the high-accuracy model was employed, the testing on the 400+ attendees with 14 reference tags is depicted as Figure 9.

The positioning accuracy was evaluated by collecting arbitrary 20 trials as Table 2 shows. The worst case (marked by *) obtained 1.36 m (m for meter) of the absolute error (Euclidean distance to the real coordinate) and 84.9% relative accuracy; the best case obtained 0.39 m of the absolute error and thus 97.8% accuracy; the average accuracy among the all trials was 92.9%. All the results were a little better than the results of LANDMARC [10]. This was mainly because (1) the conference venue had a very clean electromagnetic environment and the space inside was also broad, and (2) the RFID tags were made in new technology and the signal quality could be maintained to a stable level; those were all good for the RSS stability and the algorithm accuracy.

It should be noticed that the results in Table 2 were tested only within the rectangular area covered by the four RFID readers. The worst case (marked by *) was actually not the globally worst. The testing results outside the rectangular area showed that the worst case of the positioning accuracy could be up to 50%. However, the main focus of this paper is the entire model rather than the specific positioning algorithm; the positioning accuracy may be further improved in case of necessity.

5.2.4. Analysis. Based on the implementation and the testing results shown above, the usability, QoS, scalability, and the privacy of the location-sensing model for ESNS in this paper can be analyzed as follows.

**Usability.** The testing system corresponding to the model of this paper is simple, flexible, and scalable to deploy and configure, which was verified from the trial in the conference with 400+ attendees. The specific deployment scheme can be easily determined in the cases with or without irregular venue shapes, and the users only need to wear the small RFID tags.
tags. The trial application was also implemented as a browser-server application, which showed its flexible adaptability to different ubiquitous service applications.

QoS. We have models with different positioning accuracy prepared for different QoS/privacy scenarios. The hybrid zoning algorithm and the LANDMARC algorithm all worked well according to the trial results. The power consumption of the tag was also very small due to the testing, and it was estimated to last for 3 years by the data rate of one blink every thirty seconds.

**Scalability.** The trial system could support flexible user volume up to 500 users without any further complicated configuration and changes on the models. Based on the testing results and further theoretical analysis, the model can hopefully support up to 1000 users with the same system (the same computers, networks, and readers). The scalability of the model is promising.

**Privacy.** Considering the privacy requirements of the application for the conference ESNS, the users were allowed to configure their privacy levels. In the strictest case, the reader can also discard the sensing signals directly as long as the user set the location privacy to "not shared," which is considered to avoid any possible trace or leak of the position information beyond the physical-collection layer and lower down the privacy risks.

**6. Conclusions**

This paper presents a scalable and privacy-aware location-sensing model that could be employed by ESNS. The model consists of the architecture, the deployment model, the positioning algorithm, and the privacy control, which can meet the requirements of the usability, QoS, scalability, and privacy for a standard ESNS. We verified the model with our implemented conference-based ESNS, Find & Connect for UbiComp 2011, the analysis of the data and the trial experience show that the model is efficient and scalable. However, the positioning accuracy should also be further improved to meet more challenging requirements and the entire model should be tested much in the future work.

**Acknowledgment**

This work is funded by the State Key Development Program for Basic Research of China 2011CB302902 and NSFC 61201357.

**References**

[1] J. Burke, D. Estrin, M. Hansen et al., “Participatory sensing,” in *Proceedings of the ACM Sensys, Worldwide Sensor Web Workshop*, 2006.

[2] H. Kawaji, K. Hatada, T. Yamasaki, and K. Aizawa, “Image-based indoor positioning system: fast image matching using omnidirectional panoramic images,” in *Proceedings of the 1st ACM International Workshop on Multimodal Pervasive Video Analysis*, pp. 1–4, Firenze, Italy, October 2010.

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

[4] M. McCarthy, P. Duff, H. L. Muller, and C. Randell, “Accessible ultrasonic positioning,” *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 86–93, 2006.

[5] R. Harle, “A survey of indoor inertial positioning systems for pedestrians,” *IEEE Communications Surveys & Tutorials*, no. 99, pp. 1–13, 2013.

[6] X. Lu, C. Chia-Chih, and J. K. Aggarwal, “Human detection using depth information by Kinect,” in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW ’11)*, pp. 15–22, 2011.

[7] C. K. Schindhelm, “Evaluating SLAM approaches for microsoft kinect,” in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM ’00)*, pp. 350–362, May 2005.

[8] K. Muthukrishnan, M. Lijding, and P. Havinga, “Towards smart surroundings: enabling techniques and technologies for localization,” in *Proceedings of the 1st International Workshop on Location- and Context-Awareness (LoCA ’05)*, pp. 350–362, May 2005.

[9] P. Bahl and V. N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system,” in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM ’00)*, vol. 2, pp. 775–784, March 2000.

[10] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, “LANDMARC: indoor location sensing using active RFID,” in *Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom ’03)*, pp. 407–415, March 2003.

[11] C. Qun, L. Hua, Y. Min, and G. Hang, “RSSI ranging model and 3D indoor positioning with ZigBee network,” in *Proceedings of the IEEE/ION Position Location and Navigation Symposium (PLANS ’12)*, pp. 1233–1239, 2012.

[12] J. Schroeder, S. Galler, and K. Kyamakya, “A low-cost experimental ultra-wideband positioning system,” in *Proceedings of the IEEE International Conference on Ultra-Wideband (ICU ’05)*, pp. 632–637, September 2005.

[13] F. G. Bührer, “Ultra wide band (UWB) transmitter with configurable design for indoor positioning,” in *Proceedings of the 18th International Conference on Microwaves, Radar and Wireless Communications (MIKON ’10)*, pp. 1–4, IEEE Press, Vilnius, Lithuania, June 2010.

[14] K. Pahlavan, X. Li, and J. P. Mäkelä, “Indoor geolocation science and technology,” *IEEE Communications Magazine*, vol. 40, no. 2, pp. 112–118, 2002.

[15] K. H. Lee and S. H. Cho, “CSS based localization system using Kalman filter for multi-cell environment,” in *Proceedings of the International Conference on Advanced Technologies for Communications (ATC ’08)*, pp. 293–296, IEEE Press, Hanoi, Vietnam, October 2008.

[16] M. Duckham and L. Kulik, “Location privacy and location-aware computing,” in *Dynamic & Mobile GIS: Investigating Change in Space and Time*, J. Drummond, Ed., pp. 34–51, CRC Press, Boca Raton, FL, USA, 2006.

[17] J. Krumm, “A survey of computational location privacy,” *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.
[18] E. Kaasinen, "User needs for location-aware mobile services," *Personal and Ubiquitous Computing*, vol. 7, no. 1, pp. 70–79, 2003.

[19] G. Danezis, S. Lewis, and R. Anderson, "How much is location privacy worth?" in *Proceedings of the 4th Workshop on the Economics of Information Security*, Harvard University, Cambridge, Mass, USA, 2005.

[20] X. Zuo, A. Chin, X. Fan et al., "Connecting people at a conference: a study of influence between offline and online using a mobile social application," in *Proceedings of the 5th IEEE CPSCom Conference*, Besancon, France, 2012.
