Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 212741, 13 pages
http://dx.doi.org/10.1155/2014/212741

Research Article

Security Visiting: RFID-Based Smartphone Indoor Guiding System

Hong Zeng, Jianhui Zhang, Guojun Dai, Zhigang Gao, and Haiyang Hu

College of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China

Correspondence should be addressed to Jianhui Zhang; jhzhang@ieee.org

Received 18 June 2013; Revised 30 November 2013; Accepted 16 December 2013; Published 19 January 2014

Academic Editor: Yunhuai Liu

This paper presents a security visiting guiding system SVG composed of RFID, smart phone, and Wi-Fi signal widely available. The SVG system can provide visitors with the map of a given building, so that the visitor can easily find the target under its guide. It can also protect user's privacy location information by cryptographic two-dimension code and RFID. The two-dimension code can be easily obtained by a mobile phone and it authorizes a visitor to obtain the navigation service of SVG. The visitor receives the permission from his host and makes a date through SVG. Then, SVG will navigate both the persons to meet at any place in the building. Furthermore, this paper demonstrates and evaluates the SVG security scheme. We conduct an attacker model and test the ability of the scheme in protecting user's location security.

1. Introduction

Recently, people have achieved universal interpersonal communication with the help of modern devices, such as mobile phone and Internet. It brings huge benefits and convenience to the human relationship. However, such improvement on interpersonal communication might be abused so that the private information and property are divulged or lost. Especially, deliberate attacker or thieves always take advantage of a weak point in some open occasions. For example, some offices or labs can be arbitrarily accessed in many universities. Thus, some instrument and apparatus may often be misplaced and lost, or even be stolen sometimes. In this case, as such valuable devices may be lost, the open offices or labs will not be well used by the students. In another case, some private information, such as phone number or personal address, can be leaked when a stranger visits a host. The host may be willing to meet the stranger in a public place rather than personal addresses. Meanwhile, the host does not know the stranger and do not want to leak his personal phone number. This is another challenge.

This paper considers two scenarios: meeting stranger and managing valuable things, such as instrument and apparatus. These two scenarios seem to be not related to each other but the common point between these two scenarios is that a host meets/tracks an unknown or uncontrollable object. There are technologies to ensure that strangers can find each other by smartphones given the condition that the phone numbers are known [1]. In this paper, we address the same situation without the personal phone number being leaked. Considering another scenario, valuable objects in an open place could be easily lost. Previous work designed a tiny device equipped on valuable things, such as TV or sofa, so the tagged object can be tracked in case that it is stolen [2–4]. The proposed system will not only detect the stolen valuables, but also alarms before an object is moved away from the building. In this way, the object can be found as early as possible. Furthermore, we combine these two scenarios together and design a system to address the above challenges in these two scenarios.

In this paper, we present a novel security visiting guiding (SVG) system based on a combined system of smartphone and RFID. Based on this system, a host can meet strangers easily while his personal information will not be leaked. At the same time, the system can also manage the valuable objects so that they will not be lost. SVG consists of two parts: hardware and software. The hardware part is composed of

RFID tags, readers, smartphone, and a server. The software part is a security visiting service, which runs on the server. The server also has a database storing the information of objects, such as a device or mobile phone, and each object is also assigned a unique number. The SVG system is usually equipped in a building or a lab. Thus, the server stores the map of the building or the lab, and a computer terminal which is located at the entrance of the building. When a stranger comes into the building and wants to meet a host over there, he can register in the system from the front desk client. After he obtains the host's affirmation, the system assigns him a temporary number. SVG uses the temporary numbers and the host's number to guide both of them. Even when they are moving, SVG can suggest them the shortest path and help them meet each other as quickly as possible.

The contribution of this paper is as follows:

(i) this paper designs a security visiting guiding SVG to protect personal information while offering guiding service;

(ii) SVG combines RFID and smartphone and uses Wi-Fi signal widely available. It can also manage objects and track their position in case the they are lost;

(iii) we design a system for security visiting guiding. The system can offer visitor the map of a given building so that the visitor can conveniently find its target according to the map under the guide of SVG;

(iv) this paper demonstrates and evaluates our SVG security scheme. The attacker model is introduced to test the ability of the scheme to protect user's location security. This model uses the entropy metric to quantify the privacy. The experiment results show that the entropy under our scheme can provide a good quantitative location privacy protection for users.

In the following context of this paper, we first introduce the background and our motivation in Section 2. Section 3 surveys the related work on location and location security. We present the design of our system in Section 4, and the evaluation results of our system are presented in Section 5. The whole paper is summarized in Section 6.

2. Background and Motivation

Nowadays, strange interviewers often enter personal offices or rooms in some company office buildings and school teaching/research buildings because these buildings are open for common people. Among these visitors, some are welcomed or dated in advance, such as students who want to meet teachers in a teaching or research building. Others may be not.

Although there are sign tables to indicate the office room numbers for people who work in a building, these persons do not always stay at their offices and interviewees unfamiliar to the buildings may spend much time on looking for a specific room. The private location information of these persons was provided openly, not guaranteed to be safely used. Meanwhile some unwelcomed visiting may interrupt the normal working or even threaten the safety of these persons. Although people can date by the traditional ways including communicating with each other by emails or phone calls in advance, it will take much extra time for some welcomed and strange interviewers to find the rooms of their interviewees when the interviewers are not familiar to the structure of the building, in which their interviewers are now located.

In recent years, many works designed new location approaches for smartphone users [1, 5–9] under the indoor scenario. The common target of these previous determines the latitude/longitude of the user by using Wi-Fi, FM, and so on, which are widely available in office or school teaching/research buildings. The previous works can help an interviewer find his/her interviewee by updating their locations frequently. But the application in this paper does not need the accurate location information but the logical location, such as office room number. Previous works [10–12] designed methods to identify the logical locations (Starbucks, Walmart, and RadioShack) instead of the coordinate-based localization. Constandache et al. designed an interesting system, called *Escort*, to guide a user to the vicinity of a desired person in a public place [1]. This idea of this system *Escort* is quite similar to that of this paper and it may lead to long delay or complex calculation since it learns the walking trails of different individuals periodically. These previous works can localize the coordinate-based or logical positions for users by smartphone but did not consider the privacy protection of individual users because the personal information, including personal position and time, phone number, and so on, may be revealed and abused in the process of localization.

Existing research has explored some methods to protect the privacy of users' locations. These methods can be broadly viewed in four different approaches [13], including k-anonymity [14, 15], pseudonyms and mix zones [16, 17], path confusion [18], and hiding stars [19]. However, a person has to receive some strange interviewees sometimes in our system. In other words, a pair of trusted persons must know the location of each other. So these previous works did not meet the security requirement in our system. It motivates us to design a new system to offer the location information to authorized person and navigating one person to meet other persons meanwhile protecting the personal information during the process of localization. To ensure offering logical navigation for users while protecting their personal information, we design a system to allow authorized visiting and to prevent those unwilling visitings. This system bridges the connection between a host and an authorized visitor while protecting the hosts personal information from being revealed. Under this scenario, the system offers location information for both users to meet each other as quickly as possible. On the other hand, those unauthorized users cannot be offered localization information of both himself and the host. Our design aims to offer location and visiting service for the authorized persons while protecting their personal information by using the fare-free signal from widely available devices, such as Wi-Fi, in indoor scenario.

Nowadays, many office and teaching/research buildings are open so the personal privacy must be more carefully

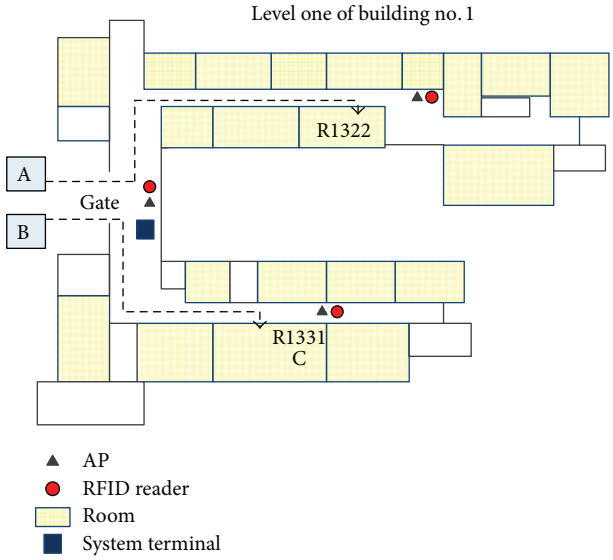


Figure 1: A visiting scenario.

protected than those enclosed. Meanwhile, our system offers location service for those authorized persons so that a visitor, especially a strange visitor, can find his host quickly. Considering a scenario as the example shown in Figure 1, a visitor B is going to visit a host in room R311. Under this scenario, there are several cases, as listed below, that may often happen. When the visitor B is a stranger, he does not know whether the host C is in his room or not at the moment he arrives at his office. B does not know C's phone number but knows his name. This case is quite common; for example, students may look for their teacher in their university. In this case, B wants to obtain the certification from C about at least two questions. Does C agree to meet B? If yes, where is C so that B can find C quickly? C may not want to reveal his personal phone number to B though he agrees to meet B. Even if B knows C's room and phone number, B may require C's agreement to meet and must know where C is now. Although C may be now in Building No.1, he will not be in the Room R1311 of this building.

Therefore, the protection of personal information is necessary and location service can offer convenience for people meeting. Our system makes better use of the indoor infrastructure, such as Wi-Fi, in office or teaching/research building since such infrastructure is widely available nowadays. Meanwhile, we explore various lightweight sensors (e.g., microphone, accelerometer, etc.) on mobile phones to enable automatic and intelligent data collection in order to help the protection of personal information and the accurate location service.

3. Related Works

3.1. Location. The problem of indoor localization has been well researched by smartphone in recent years [1, 5–7]. Since the GPS information is hard to be available under the indoor scenario, techniques based on observation of signals from radio beacons, including Wi-Fi [20], cellular base stations (such as GPRS), or acoustic background spectrum [6], showed the most promise.

Tarzia et al. proposed an ambient sound fingerprint called the acoustic background spectrum (ABS) to determine a mobile phone's indoor location even when Wi-Fi infrastructure is unavailable or sparse [6].

Constandache et al. designed and implemented Escort, a system that guides a user to the vicinity of a desired person in a public place [1]. They only used an audio beacon, randomly placed in the building, to enable a reference frame and did not rely on GPS, Wi-Fi, or war-driving but accelerometer and compass measurements on smartphones. Similar works were also given to delete the reliance on Wi-Fi infrastructure and war-driving [21, 22].

Breaking away from coordinate-based localization, authors in [10–12] propose ways to identify logical locations (Starbucks, Walmart, and RadioShack), as opposed to physical coordinates (as in GPS). The rationale is that a large class of applications do not care about the latitude/longitude of the user; instead they desire to know the "place," where the user is located. These and several other works [23, 24] emphasize the broad and evolving nature of localization technology, driven primarily by the fast changing landscape of mobile, pervasive, people-centric computing.

There are lots of works using the signal of Wi-Fi to locate the position of users or clients [20, 25–31]. Another works analyzed the localization of the users in RFID systems [7, 32, 33].

Chen et al. proposed a framework that supports the group guiding service; that is, several members followed the track of a leader in a mixed group by RFIDs and wireless sensor networks [34]. A response mechanism will be built between leader and members, and a group guiding protocol is presented. The design enables reliable group guiding at low cost and low traffic load.

Nowadays, rfid-based positioning methods have been proposed. Wang and Katabi presented the first RFID positioning system to pinpoint the exact location of a tagged object combined with the synthetic aperture radar (SAR) and dynamic time warping (DTW) techniques [35]. Xu et al. designed and implemented an RF-based device-free passive localization strategy using active RFID nodes and reached 97.2 percent accuracy and 0.36 meters average error distance [36].

3.2. Location Security. Many works have been put on protecting the security of individual location [13–16, 19, 37, 38].

k-anonymity provides a form of plausible deniability by ensuring that the user cannot be individually identified from a group of *k* users [14]. Alternate formulations such as *CliqueCloak* wait until at least *k* different queries have been sent from a particular region [15].

Gruteser and Liu provided pseudonyms and mix zones method, by which each new location is sent to the LBS with a new pseudonym, and then the LBS may have difficulty following a user [16]. However, frequent updating may expose

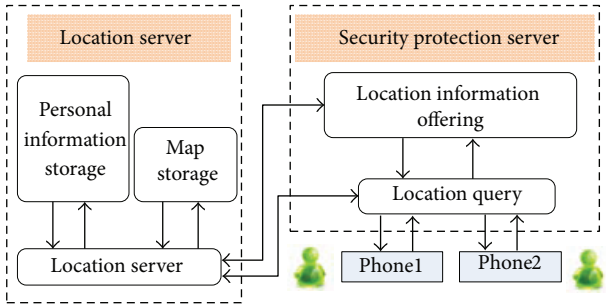


Figure 2: The architecture of SVG.

a pattern of closely spaced queries, allowing one to easily follow the user [17].

Hoh et al. extended the method of mix zones to path confusion by resolving the same-place same-time problem [18]. Path confusion will decide to not release the users' locations at all if insufficient anonymity has been accumulated after an interval. But it poses the risk that, for significant intervals of time, users' locations will not be exposed to the LBS. Naturally, service from the LBS will be unavailable for this entire duration.

When these previous methods try to obscure the user's path by hiding parts of it, Meyerowitz and Choudhury obscured the user's location by surrounding it with other users' paths [19]. In order not to require changing the LBS server architecture and third party privacy-protection servers, Shokri et al. developed a scheme MobiCrowd that allowed LBS users to reduce their exposure while they continued to receive the location context information that they need [39]. MobiCrowd achieved this by leveraging on peer collaboration: the user can get information from nearby users and can thus avoid getting exposed to the LBS server. This paper adopts a quite simple and effective method to protect users' location and information by hiding the individual information, which is quite different from previous works.

4. SVG System Design

This section describes the structure of our SVG system and presents techniques to deal with the challenges described in Section 1.

4.1. System Overview. Our SVG system is composed of the following components shown in Figure 2.

4.1.1. Location Server. As shown on the left side of Figure 2, the location server contains three functions: localization service, personal information, and building structure storage. The server stores the digital maps of building structures, which are preprocessed and stored in the server in advance. The personal information of the persons, who work in the building (such as phone or room number), can be stored in advance or updated online. The server also provides localization service to those authorized persons.

4.1.2. Security Protection Server. The security protection server provides the service to protect the private information for the people, whose personal information was stored in the location server and the location of both visitors and their hosts. It contains a security protection mechanism to establish the connection between a visitor and the server by one time of hand-shaking. The visitors, who agree to have meetings by their hosts or were registered in the location server, are authorized to obtain the localization service. The mechanism ensures that the authorized users can localize themselves or their hosts so that they can know their location and find their hosts as soon as possible.

4.1.3. Security Protection Mechanism. In many common visiting, the personal information, such as his current location and phone number, is reluctant to be shared. In our system, we design a QR code-based mechanism to protect personal information and to authorize visitors to download the building map from the location server to personal smartphone. We hide the personal information in a QR code so that each individual has his corresponding code. The QR code form is shown in Figure 3(a) and the generated two-dimensional code picture is shown in Figure 3(b).

These personal information and their codes are stored in the location server. On the other hand, the building map is previously drawn and stored in this location server. When a visitor is authorized by his host through the QR code offered on the terminal at the front door in Figure 1, he can download the building map and obtain the location serve.

4.1.4. System Security Scheme. Meyerowitz and Choudhury [19] divided the testing area into regular 10 m∗10 m pixel and designed and implemented a "Cachecloak" security privacy engine to protect the mobile cars' location information from being attacked by hostile. Our SVG system scheme adopts the similar method to protect the hosts' location information besides the above RFID and QR code. Each floor of the building was partitioned into two kinds of cells: bidirectional corridor as one kind of cell and the intersection among the corridors and stairs as another kind. Each cell is allocated a 3∗3 historical matrix C, and as one of the elements of the matrix. The initial data of the matrix can come from the historical database from multiple users. Each element c_{ij} of the matrix means the number of times entering from cell i and exiting to cell j.

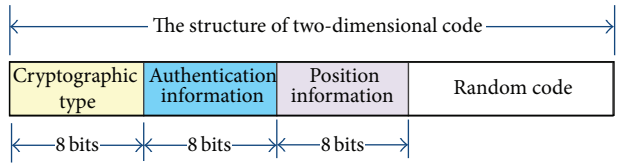
Therefore, given the entering cell i, the conditional probability exiting for cell j is

$$p(j \mid i) = \frac{c_{ij}}{\sum_i c_{ij}}. \quad (1)$$

Then, the probability exiting for cell j is

$$p(j) = \frac{\sum_j c_{ij}}{\sum_i \sum_j c_{ij}}. \quad (2)$$

Through the scheme, we can forecast the most possibility of arriving at cell j. The entire location information will then be sent to the server.



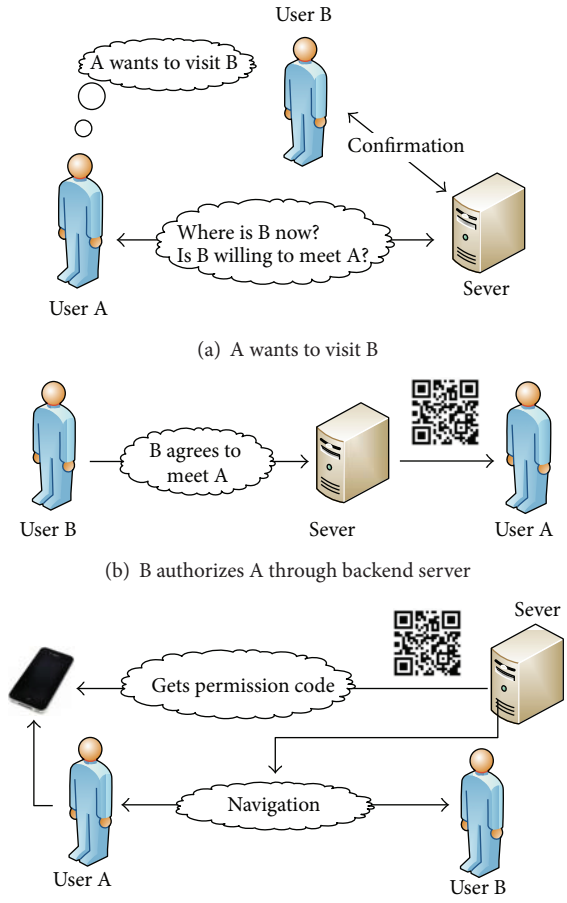
(a) Two-dimensional code form

(b) The two-dimensional code

FIGURE 3: The structure of two-dimensional code.

4.1.5. Visitor and Host Users. Host users refer to those users registered in the location server, who work in the building. Visitor user refers to any person, who is going to visit some hosts in the building or just want the localization service. Naturally, a visitor user initiates a meeting by querying his host through the security protection server.

Next, we give an example in Figure 4 and demonstrated the detail work process of our system. In the scenario of this example, user A wants to visit B and is not sure where B is now. So he wants to know where B is now and how to find him. If A is not familiar with the building where B works, it would be more difficult for A to find B. Our system can offer service to A and help him find B quickly by a terminal, which is preciously placed at the entrance of the building as shown in Figure 1. Through the terminal of our system, A asks B's confirmation to meet as shown in Figure 4(a). During this process, in order to protect B's personal information (e.g., personal phone number), A is not sure whether B will want to meet him or not and he does not know the accurate position B will be located at. Thus, A can query through the terminal connecting to a server, which contains the location server and security protection server. The security protection server then sends a message to B through the Wi-Fi APs (as shown in Figure 4(a)). If B agrees to meet A, the security protection server feeds back to A and offers A an encrypted two-dimensional code (as shown in Figure 4(b)). Only A can use the camera in his smartphone to get B's information by scanning the picture and inputting his password. Others cannot unlock the picture without the password.



(a) A wants to visit B

(b) B authorizes A through backend server

(c) A gets the permission

FIGURE 4: The mechanism of security visiting.

4.2. Hybrid Localization. In indoor environment, GPS signal is weak or unprocurable so those GPS-based localization methods are not precise enough. Other localization methods, such as cellular base stations (such as GPRS) or acoustic background spectrum [6], can offer precise location information for users. But they can only offer location for individuals and cannot show the relative positions of several persons. For example, when A tries to find B, the quite useful information for A is B's position relative to A. In the scenarios of visiting, the precision of these above methods is relatively low. In our system, we combine precious localization methods and help users to find each other at two stages. At the first stage, we use Wi-Fi-based localization methods [30, 31] to guide visitors

to get close to each other when the distance between them is long. At the second stage, Wi-Fi-RFID-combined method [34] is used to shorten the searching time when host and visitor are close to each other. In this line-of-light range, it is quite easy to find each other.

4.3. Navigation Time. The navigation time is an important metric to measure the performance of our system. Users are willing to find their host in a time as short as possible. The navigation time, in this paper, is defined as the interval from the moment a visitor is authorized to access our system at the terminal to the time that he finds his host.

5. System Implementation and Evaluation

We implement a prototype system on the Android platform by using two kinds of experiment methods in the experiment scene. We test and evaluate the system performance. We first present the experiment setup in Section 5.1, then we describe the experiment scene in Section 5.2. Experiment results are given in Section 5.3. We present the overall performance of searching time using the system comparing to that not using the system in Section 5.4. Finally, the evaluation of privacy quantization based on the attacker model is presented in Section 5.5. The following subsections give more details about the experiment methodology and findings.

5.1. Experiment Setup. As shown in Figures 5(a) and 5(b), we implement the application on the Android 2.3 platform with ZTC mobile phone, RFID transceiver GZ100-NR01, and RFID perception-location tag WS-CT-06. The ZTC has a 192 MB RAM and 528 MHz 7201 processor. The GZ100-NR01, using 2.4 GHz wireless communication frequency, has more than 30 m wireless communication distance. The WS-CT-06 is ultra-low power RFID tag, its power transmission is less than 1 mW, and communication distance reaches more than 40 m.

We implement the localization and security protection application on the DELL PowerEdge 2950 PC server with 2 GB memory and Intel Xeon E5405 processor. The sever established communication connections between terminal and server and server and mobile phone by socket technique to provide five kinds of serve, including foreground serve, mobile phone serve, RFID serve, data encryption, and database management, as shown in Figure 6.

5.1.1. Foreground Serve. Foreground serve requests message from terminal and interacts information between server and terminal. It uses user-defined communication protocol and the communication port number is 8000. Foreground serve responds to the request of terminal by command-line format "command-XX∗XX∗".

It has three types of commands: (1) find-AA∗BB∗, (2) code-XX∗, and (3) pic-.

In "find-AA∗BB∗" command, "AA" describes the information of host, such as name and RFID ID number. "BB" represents the information of visitor, such as visitor's name and main content of visiting. "∗" means the space between AA and BB. The command is to represent the procedure in which the visitor wants to visit the host; he or she should input some information listed above, and the backend server will analyse the information according to the command format and feed back the search result to the visitor using the returned value of the finding command. The find command has five returned values: −1, 0, 1, 2, and 3. "−1" means that the host is offline, "0" means search failure, "1" means that the host refuses meeting, "2" means successful search and the visitor is ready to input encrypted key, and "3" means the server receives the encrypted key successfully and is ready to send encrypted two-dimensional code picture to the visitor.

In "code-XX∗" command, "XX" means the encrypted key, the command tells the server that the visitor will send the encrypted key to it and anyone else will not get the information of the two-dimensional code picture through his mobile phone without the encrypted key.

"pic-" command shows that the server will send the two-dimensional code picture with encrypted key to the terminal, and the visitor can get the two-dimensional code picture through his/her mobile phone's camera by the self-designed Android application software.

5.1.2. Mobile Phone Serve. Mobile phone serve processes the data interactions between the server and mobile phone, including mobile receiving command from the server or updating data to it. The default communication port number is 6000. The function provided by the mobile phone serve is to realize the control to mobile phone. There is only two commands: Call and Error. The "Call" command tells the host user that there is a visitor who wants to visit him/her and requests the host user to authorize whether he/she is allowed to visit or not. The "Error" command is only a debug command which is called only when the application of the mobile phone serve goes wrong.

5.1.3. RFID Serve. RFID serve receives the tag information such as the RFID transceiver's ID and tag's ID number. The information will provide the help for computing the host's location; the default port number is 6666. The format of received information is as follows:

<RFID Transceiver ID><TAG ID number1><TAG ID number2> ⋯ <TAG ID NUMBERN>.

5.1.4. Data Encryption. The system will encrypt the host's location information by means of two-dimensional code through data encryption model; the two-dimensional code picture is less than 4 MB and can only be recognized by the visitor who knows the encrypted key; we use the UTF-8 coding mode to encrypt the key.

5.1.5. Database Management. The database management model stores and manages the basic information, including name, phone number, RFID tag's ID number, and two-dimensional code picture.

5.2. Experiment Scenario. We do our experiments at building no. 1 at the campus of Hangzhou Dianzi University. The

(a) Mobile phone (b) GZ100-NRO1 and WS-CT-06

Figure 5: Mobile phone and RFID.

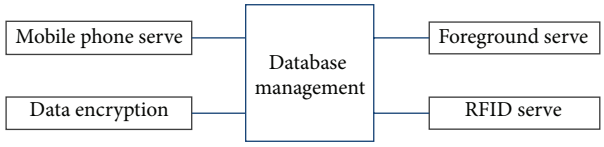


Figure 6: Five kinds of serve of the backend server.

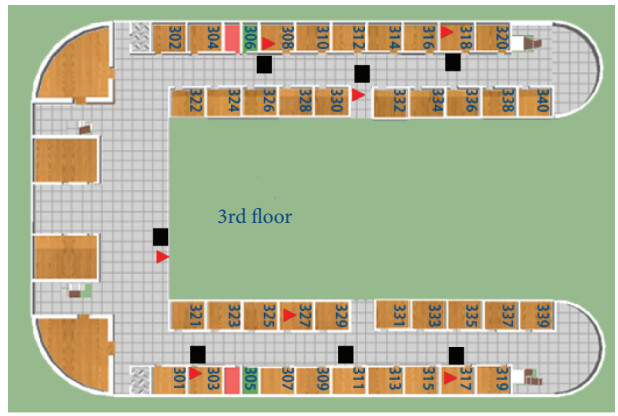


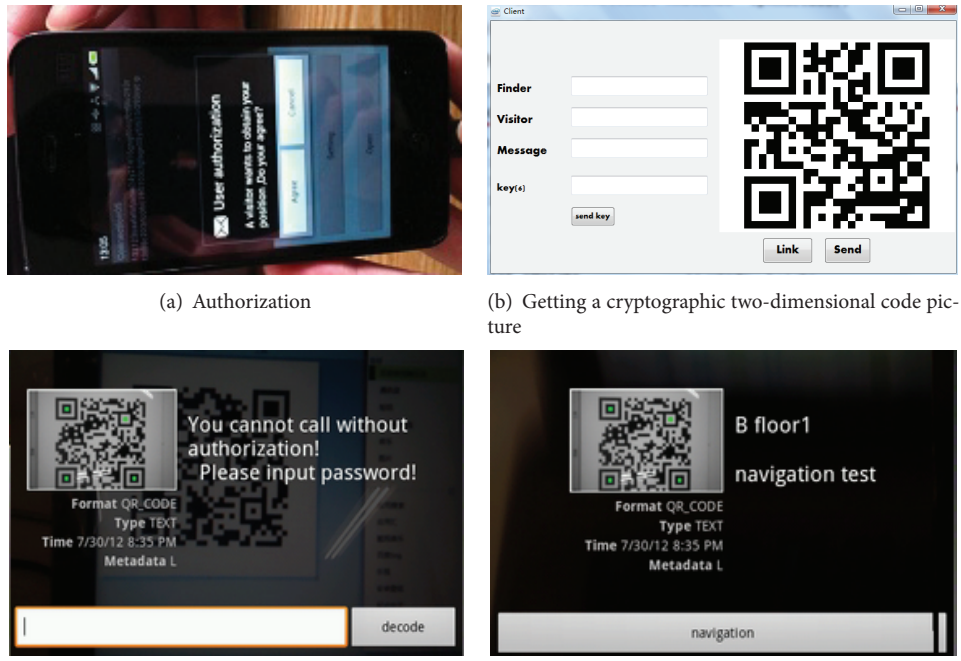
Figure 7: The plane structure of each floor.

building is U-shaped, where the north rooms' number of the building is even, and the south is odd. The structure of each floor of the building is the same. There are stairs on both north and south sides and the elevator lies in the south. To fairly undertake the experiments, the volunteers begin to find the host by stairs instead of elevator, and we count the consumed time by stopwatch. Figure 7 shows the plane structure of each floor. We use existing base stations (Δ) and place several RFID readers (□); the terminal computer is placed at the entrance hall. First, an access request by the visitor was sent to the host; after the host approved it (as shown in Figure 8(a)), the server would send a cryptographic two-dimensional code picture to the foreground (in Figure 8(b)); the visitor inputed the password (in Figure 8(c)) and decoded the two-dimensional code picture (in Figure 8(d)) to get the position information of the host.

5.3. Experiment Results. We construct two kinds of experiment scenarios: one is that the host is in one room and his or her position is unchanged, the other one is that the host's position is dynamically changed. Some volunteers are familiar with the host, and the others are unfamiliar. They can search the host by the host's name or his/her RFID tag ID number. We have done two groups of experiments, respectively, in each of scenarios, which are (1) the host's friends want to find him/her, but they are not familiar with the building; (2) some strangers want to find the host and they are not familiar with the building too. To eliminate accidental factors, several runs of the same experiments are carried out in our work.

5.3.1. The First Class Experiment. The position of the host user, C, is unchanged in every experiment. Two volunteers A and B want to visit C at the same time; they are both familiar with C, but are not familiar with the building and do not know where C is. A and B begin to search for C from the entrance hall at the same time. A uses the system, and inputs C's name through the terminal application to find C and B does not use the system. We compare with the time needed to find C for A and B. We will do several experiments by changing the static position of C.

5.3.2. The Second Class Experiment. The position of C is unchanged in every experiment. Another two volunteers D and E want to visit C at the same time, but they are both



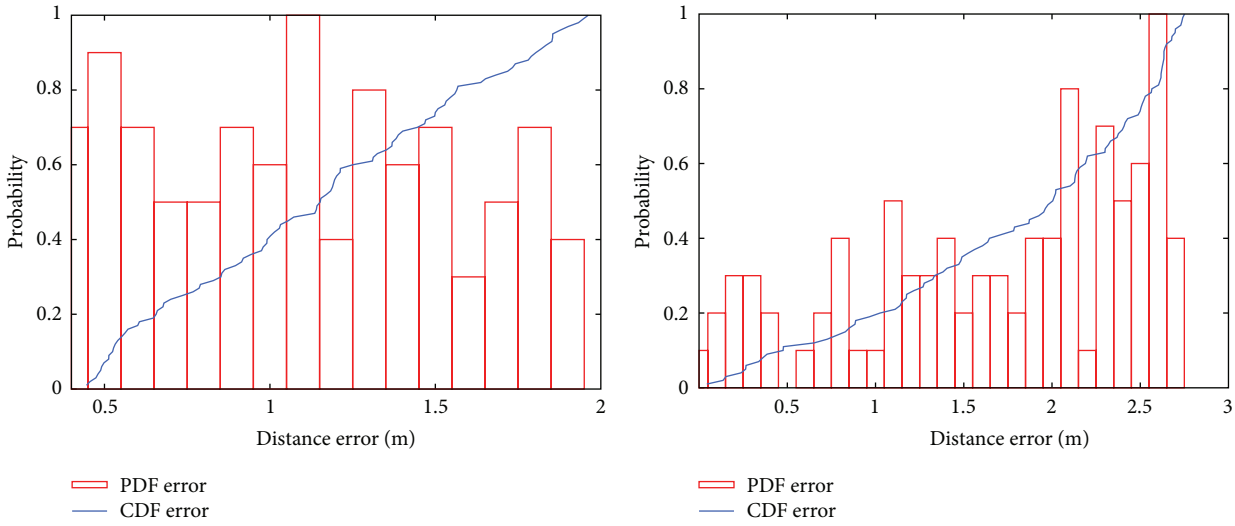
(a) Authorization

(b) Getting a cryptographic two-dimensional code picture

(c) Inputting password

(d) Decoding and acquiring the navigation information

Figure 8: The system work flow.



(a) Wireless sensor network laboratory

(b) Corridor out of wireless sensor network laboratory

Figure 9: PDF and CDF error of localization in different indoor environments.

strangers to C and do not know where C is. D and E begin to search for C from the entrance hall at the same time. D uses the system and inputs C's RFID tag number through the terminal application to find C and E does not use the system. We compare with the time needed to find C for D and E.

5.3.3. The Third Class Experiment. The position of C is changed dynamically in every experiment. Two volunteers A and B want to visit C at the same time, they are both familiar with C, but are not familiar with the building and do not know where C is. A and B begin to search for C from the entrance hall at the same time. A uses the system and inputs C's name in the foreground application to find C and B does not use the system. We compare with the time needed to find C for A and B.

5.3.4. The Fourth Class Experiment. The position of C is changed dynamically in every experiment. Another two volunteers D and E want to visit C at the same, but they are both strangers to C and do not know where C is. D and

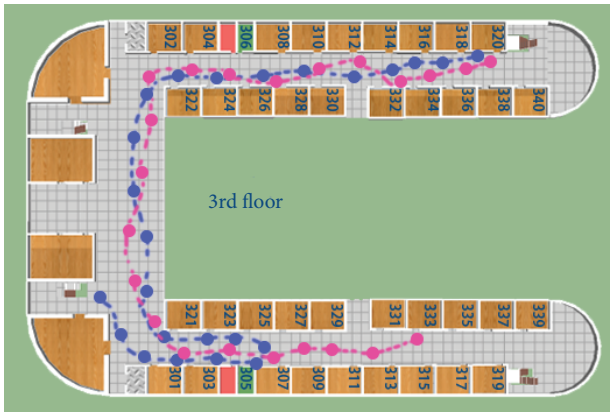


Figure 10: Localization and searching progress. Red points are the location of the host. Blue points are the visitor's location.

E begin to search for C from the entrance hall at the same time. D uses the system and inputs C's RFID tag number in the foreground application to find C and E does not use the system. We compare with the time needed to find C for D and E.

5.4. Performance Evaluation

5.4.1. Localization Accuracy in Different Places. First, we use the APs placed in the same room to measure the localization accuracy in the same room. And then, the same experiment is done in the corridor by the off-the-shelf APs deployed in different rooms and corridor. We specially take into account both the complicated multipath effect and the shadowing fading brought by wall shield. We plot the probability and cumulative distribution of localization error across 10 positions by FILA method [30], as shown in Figures 9(a) and 9(b). The average error is about 1.5 m and the maximum error is less than 3 m.

5.4.2. Searching Time and Efficiency. We collect the real time-consuming data based on the above experiments and present the final performance evaluation result. Figure 10 shows the real application of the system when the host's position is changed. After the visitor arrives at the place near room 325, he finds that the host has moved to room 320 by his smartphone application, so he changes his route and reaches the appropriate place to meet the host. Figures 11 and 12 show the experiments result and performance analysis. Figures 11(a) and 11(c) show the time needed for familiars and strangers. Figures 11(b) and 11(d) show the efficiency improvement of the first and second class searching by using the system. The time needed and efficiency performance of the third and fourth class searching are shown in Figure 12.

When the host's position is unchanged, Figure 11(a) shows the time needed that familiars want to find the host in the building without SVG versus with SVG by inputting the host's name. In Figure 11(b), the average searching efficiency is increased to 25 percent. When strangers want to find someone in the building without the system, we can find in Figure 11(c) that it will need more time comparing to Figure 11(a), if both strangers and familiars use the SVG system, the searching time needed is almost the same, and Figure 11(d) shows that there is about 35 percent efficiency improvement for strangers searching with the system. From Figures 11(a) and 11(c), we can find that if familiars and strangers use the SVG system for positioning and searching, the time needed is almost invariant, but if not, the searching time will be significantly increasing in doing the same thing, and the farther the host is from the entrance hall, the more time it will take if we do not use the SVG system.

But when the position of the host is changed dynamically, Figure 12(c) shows that it will take more time to find the host without the system than Figures 11(a) and 11(c) for familiars and strangers, and the time needed is slightly increased by using the system compared to Figures 11(a) and 11(c). When the position changed smoothly, such as in the same floor, our SVG system needs less time to find the host while the system without SVG needs more. On the other hand, for the strangers, when the position of the host changes greatly, the time needed in the system using SVG will be much lower than the systems without SVG. From Figures 12(b) and 12(d), we can find that there is about 45 percent increase of searching efficiency performance, respectively, by the SVG system.

From Figures 11(a), 11(c), 12(a), and 12(c), we can find that when the destination where the visitor wants to find is near to the foreground, such as room 105 on the first floor, it took almost the same time for strangers and familiars to get to the destination. But if the destination is far from the foreground, the strangers will spend more time without the SVG system. At the same time, we also find that there are some dots far from the curves in Figures 11 and 12; it means that it is deviated from our expected time. There are some influential factors such as Wi-Fi connection quality, two-dimensional code pictures size, and communication distance. First, in the building, Wi-Fi communication often disconnects and it will make the communication quality between the terminal and server and server and visitor become abnormal. Second, when the two-dimensional code picture size comes close to 4 M bytes, it will take more time to transmit the picture from the server to the terminal.

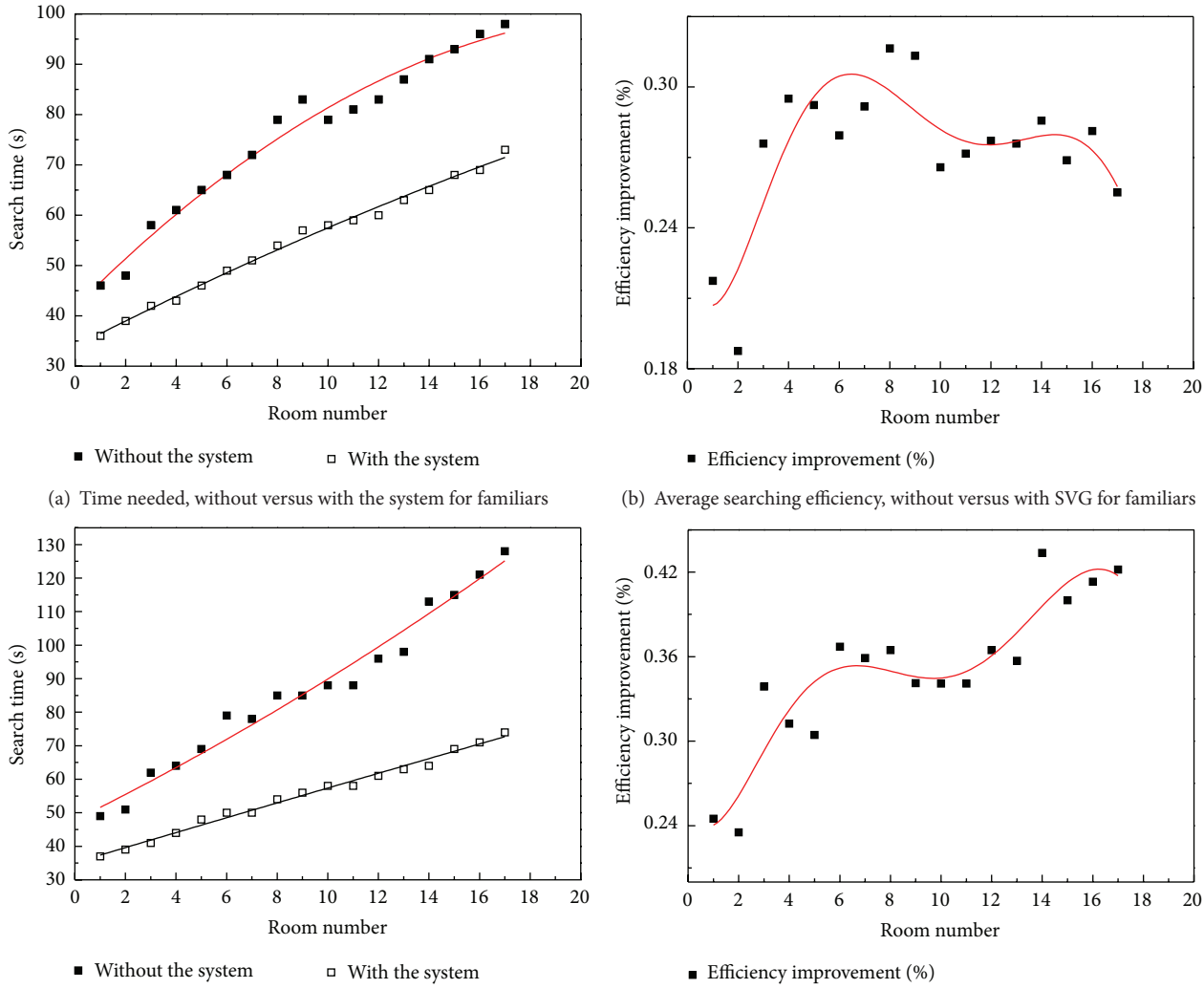
5.5. Attacker Model and Privacy Metrics

5.5.1. Attacker Model. We suppose that the attacker has access to the same historical matrix C. First, we associate a probability vector $\vec{p}(x, y)$ with each cell existing in the map. The three elements of $p_k(x, y)$ $(k = 1, 2, 3)$, as shown in (3), represent the probability that one user entered from side k to cell (x, y),

$$p_k(x, y) = \frac{\sum_j c_{kj}(x, y)}{\sum_i \sum_j c_{ij}(x, y)}. \quad (3)$$

Now, we define a transition probability $P(x, y)$, which means the probability that cell (x, y) reaches cell (x', y') from one side of cell (x, y). Then, the $P(x, y)$ can be expressed by

$$P(x, y) = p_k(x, y). \quad (4)$$



(a) Time needed, without versus with the system for familiars

(b) Average searching efficiency, without versus with SVG for familiars

(c) Time needed, without versus with SVG for strangers

(d) Average searching efficiency, without versus with SVG for strangers

FIGURE 11: The host's position is unchanged.

Through the attacker model, the attacker will determine the possibility that the user might go in any specific direction.

5.5.2. Privacy Metrics. A trace-based simulation tool VANETMobiSim [19] was brought to simulate the realistic scene of our building by the SVG security scheme. The existing map of the building was loaded into VANETMobiSim; each floor is divided into five cells and has six paths. The location information is stored in the trace file of VANETMobiSim.

We use the location entropy to quantify privacy based on the attacker model. The location entropy S is defined as the number of bit as follows:

$$S = -\sum_{(i,j)} P(x, y) \log_2 P(x, y). \quad (5)$$

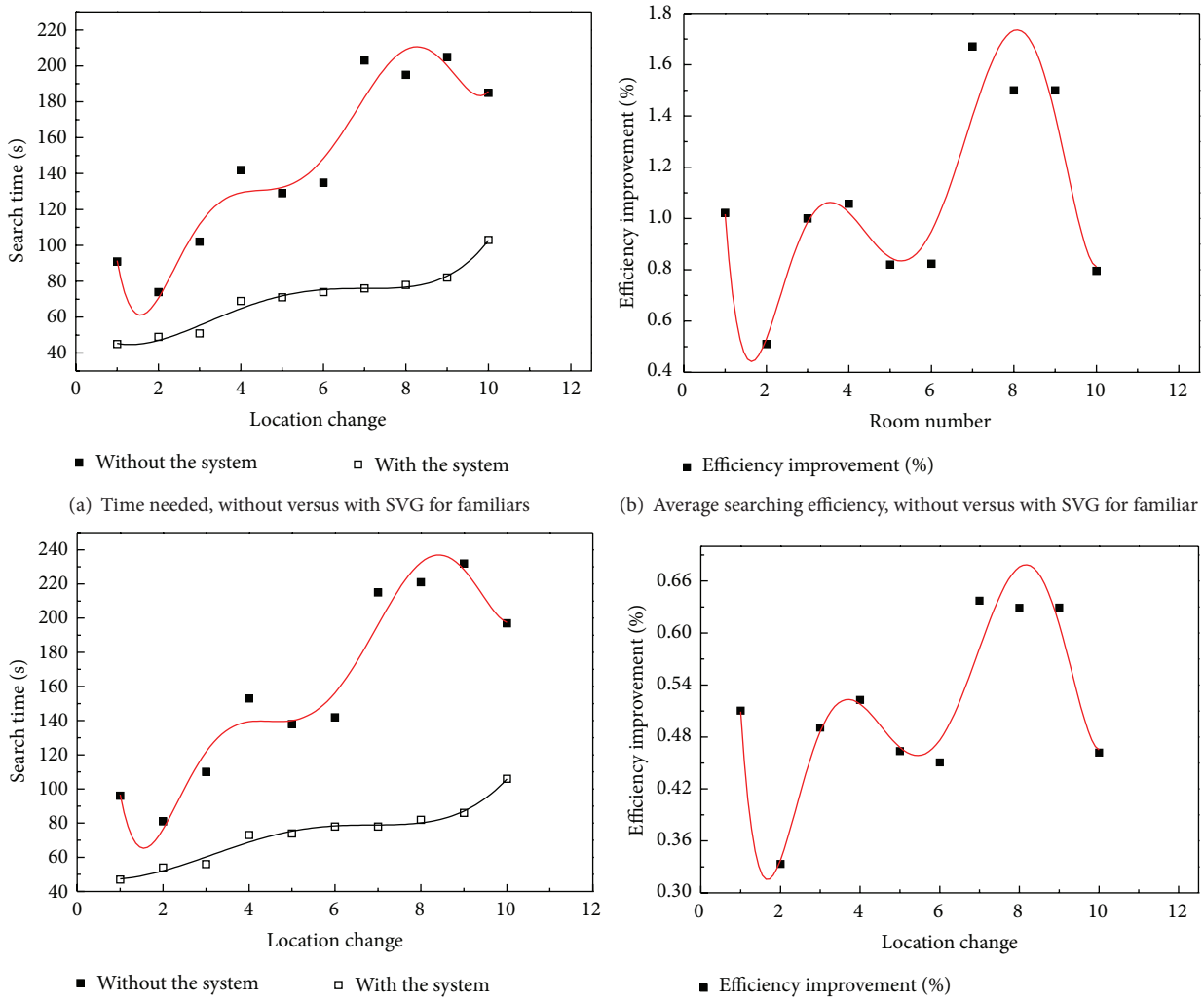
Entropy is valuable for location privacy because it gives a precise quantitative performance of the attacker's uncertainty. 2^S is easy to understand the different place where the user will be. It will give the attacker more difficulty in acquiring the location information of the user when the value of S increases.

Five nodes, randomly placed at the map, had been used to test the performance of our SVG security scheme for 20 minutes, as shown in Table 1. The simulation results show that the mean value of the S is still less by 6 bits under our SVG scheme and has notable increasing after the system is under attack for 5 minutes. It is difficult for the attacker to know where the user is, because he would find that it will spend much more time to get the correct location information among 64 different information.

In our future works, we will continue to construct a more stable communication network and improve the network transmission quality. We will try to use the 3G network to improve the network throughput.

6. Conclusion

This paper has presented a prototype SVG system using Wi-Fi, RFID, and commodity mobile phones. The proposed system provides cost-efficient solutions to indoor guiding and security visiting. We comprehensively evaluate the system



(a) Time needed, without versus with SVG for familiars

(b) Average searching efficiency, without versus with SVG for familiar

(c) Time needed, without versus with SVG for strangers

(d) Average searching efficiency, without versus with SVG for strangers

Figure 12: The host's position is changed dynamically.

Table 1: Location entropy.

Time (minute)	5	10	15	20
Location entropy (bit)	5.5124	5.6293	5.9511	5.9526

deployed on the Android platform. Through the experiments, the evaluation results demonstrate that our system can shorten the searching time and protect user's privacy.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the Major Program of the National Natural Science Foundation of China (NSFC) under Grant no. 61190113, the Young Program of NSFC under Grant no. 61003298, the Zhejiang Provincial Natural Science Foundation under Grant nos. Y1101336 and LY12F02005, and the open funding of the National Key Lab of Sonar Science and Technology in Hangzhou City under Grant no. KYB070512005.

References

[1] I. Constandache, X. Bao, M. Azizyan, and R. R. Choudhury, "Did you see Bob?: human localization using mobile phones," in *Proceedings of the 16th Annual International Conference on Mobile Computing and Networking (MobiCOM '10)*, pp. 149–160, Chicago, Ill, USA, September 2010.

[2] B. Thorstensen, T. Syversen, T.-A. Bjørnvold, and T. Walseth, "Electronic shepherd—a low-cost, low-bandwidth, wireless network system," in *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys '04)*, pp. 245–255, Boston, Mass, USA, 2004.

[3] H. T. Zhang, S. J. Tang, X. Y. Li, and H. D. Ma, "Tracking and identifying burglar using collaborative sensor-camera networks," in *Proceedings of the 31th Annual IEEE International Conference on Computer Communications (INFOCOM '12)*, pp. 2596–2600, Orlando, Fla, USA, March 2012.

[4] X. Mao, S. Tang, X. Xu, M. Li, and H. Ma, "iLight: indoor device-free passive tracking using wireless sensor networks," in *Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM '11)*, pp. 281–285, Shanghai, China, April 2011.

[5] Z. Zhang, X. Zhou, W. Zhang et al., "I am the antenna: accurate outdoor AP location using smartphones," in *Proceedings of the 17th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '11)*, pp. 109–120, Las Vegas, Nev, USA, September 2011.

[6] S. P. Tarzia, P. A. Dinda, R. P. Dick, and G. Memik, "Indoor localization without infrastructure using the acoustic background spectrum," in *Proceedings of the 9th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '11)*, pp. 155–168, Washington, DC, USA, July 2011.

[7] C. Wang, H. Wu, and N.-F. Tzeng, "RFID-based 3-D positioning schemes," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1235–1243, Anchorage, Alaska, USA, May 2007.

[8] H. Wang, S. Sen, A. Elgohary, M. Farid, M. Youssef, and R. R. Choudhury, "No need to war-drive: unsupervised indoor localization," in *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pp. 197–210, Low Wood Bay, UK, June 2012.

[9] Y. Chen, D. Lymberopoulos, J. Liu, and B. Priyantha, "Fm-based indoor localization," in *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pp. 169–182, Low Wood Bay, UK, June 2012.

[10] M. Azizyan, I. Constandache, and R. R. Choudhury, "Surroundsense: mobile phone localization via ambience fingerprinting," in *Proceedings of the 15th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '09)*, pp. 261–272, Bejing, China, September 2009.

[11] N. Ravi and L. Iftode, "Fiatlux: fingerprinting rooms using light intensity," in *Proceedings of the 5th International Conference on Pervasive Computing (ICPC '07)*, 2007.

[12] N. Ravi, P. Shankar, A. Frankel, A. Elgammal, and L. Iftode, "Indoor localization using camera phones," in *Proceedings of the 7th IEEE Workshop on Mobile Computing System and Applications (WMCSA '06)*, pp. 1–7, Orcas Island, Wash, USA, April 2006.

[13] Y. Feng, P. Liu, and J. Zhang, "A mobile terminal based trajectory preserving strategy for continuous querying LBS users," in *Proceedings of the 8th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '12)*, pp. 92–98, Hangzhou, China, May 2012.

[14] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[15] B. Gedik and L. Liu, "Location privacy in mobile systems: a personalized anonymization model," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, pp. 620–629, Columbus, Ohio, USA, June 2005.

[16] M. Gruteser and X. Liu, "Protecting privacy, in continuous location-tracking applications," *IEEE Security & Privacy*, vol. 2, no. 2, pp. 28–34, 2004.

[17] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in *Security in Pervasive Computing*, vol. 3450 of *Lecture Notes in Computer Science*, pp. 179–192, 2005.

[18] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 161–171, Alexandria, Va, USA, November 2007.

[19] J. Meyerowitz and R. R. Choudhury, "Hiding stars with fireworks: location privacy through camouflage," in *Proceedings of the 15th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '09)*, pp. 345–356, Beijing, China, September 2009.

[20] D. Madigan, E. Elnahrawy, R. P. Martin, W.-H. Ju, P. Krishnan, and A. S. Krishnakumar, "Bayesian indoor positioning systems," in *Proceedings of the 24th Annual Joint of the IEEE Computer and Communications Societies (INFOCOM '05)*, vol. 2, pp. 1217–1227, Miami, Fla, USA, March 2005.

[21] S. P. Tarzia, R. P. Dick, P. A. Dinda, and G. Memik, "Sonar-based measurement of user presence and attention," in *Proceedings of the 11th ACM International Conference on Ubiquitous Computing (UbiComp '09)*, pp. 89–92, Orlando, Fla, USA, October 2009.

[22] I. Constandache, R. R. Choudhury, and I. Rhee, "Towards mobile phone localization without war-driving," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, San Diego, Calif, USA, March 2010.

[23] G. Ananthanarayanan, M. Haridasan, I. Mohomed, D. Terry, and C. A. Thekkath, "StarTrack: a framework for enabling track-based applications," in *Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '09)*, pp. 207–220, Krakow, Poland, June 2009.

[24] Y.-C. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm, "Accuracy characterization for metropolitan-scale Wi-Fi localization," in *Proceedings of the 3rd ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '05)*, pp. 233–245, Seattle, Wash, USA, June 2005.

[25] A. P. Subramanian, P. Deshpande, J. Gao, and S. R. Das, "Drive-by localization of roadside WiFi networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 718–725, Phoenix, Ariz, USA, April 2008.

[26] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka, "You are facing the Mona Lisa: spot localization using PHY layer information," in *Proceedings of the 10th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pp. 183–196, Low Wood Bay, UK, June 2012.

[27] K. Lin, A. Kansal, D. Lymberopoulos, and F. Zhao, "Energy-accuracy aware localization for mobile devices," in *Proceedings of the 8th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '10)*, pp. 1–4, San Francisco, Calif, USA, June 2010.

[28] I. Constandache, S. Gaonkar, M. Sayler, R. R. Choudhury, and L. Cox, "Enloc: energy-efficient localization for mobile phones," in *Proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM '09)*, pp. 2716–2720, Rio de Janeiro, Brazil, April 2009.

[29] T. Jin, G. Noubir, and B. Sheng, "WiZi-Cloud: application-transparent dual ZigBee-WiFi radios for low power internet access," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '11)*, pp. 1593–1601, Shanghai, China, April 2011.

[30] K. Wu, J. Xiao, Y. Yi, M. Gao, and L. M. Ni, "FILA: fine-grained indoor localization," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '12)*, pp. 2210–2218, Orlando, Fla, USA, March 2012.

[31] C. Feng, W. S. A. Au, S. Valaee, and Z. Tan, "Compressive sensing based positioning using RSS of WLAN access points," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, San Diego, Calif, USA, March 2010.

[32] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: indoor location sensing using active RFID," *Wireless Networks*, vol. 10, no. 6, pp. 701–710, 2004.

[33] R. Tesoriero, J. Gallud, M. Lozano, and V. Penichet, "Using active and passive RFID technology to support indoor location-aware systems," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 2, pp. 578–583, 2008.

[34] P.-Y. Chen, W.-T. Chen, Y.-C. Tseng, and C.-F. Huang, "Providing group tour guide by RFIDs and wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 3059–3067, 2009.

[35] J. Wang and D. Katabi, "Dude, where's my card?: RFID positioning that works with multipath and non-line of sight," in *Proceedings of the ACM International Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM '13)*, pp. 51–62, Hong Kong, China, August 2013.

[36] C. Xu, B. Firner, Y. Zhang, R. Howard, and J. Li, "Poster: statistical learning strategies for RF-based indoor device-free passive localization," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (SenSys '11)*, pp. 365–366, Seattle, Wash, USA, November 2011.

[37] Z. Zhu and G. Cao, "APPLAUS: a privacy-preserving location proof updating system for location-based services," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '11)*, pp. 1889–1897, Shanghai, China, April 2011.

[38] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," in *Proceedings of the International Conference on Computer Communications (INFOCOM '12)*, pp. 729–737, Orlando, Fla, USA, March 2012.

[39] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, "Collaborative location privacy," in *Proceedings of the 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '11)*, pp. 500–509, Valencia, Spain, October 2011.