Noname manuscript No.
(will be inserted by the editor)

Privacy Preserving in Indoor Fingerprint Localization and Radio Map Expansion

Amir Mahdi Sazdar · Nasim Alikhani · Seyed Ali Ghorashi · Ahmad Khonsari

Received: date / Accepted: date

Abstract Preserving privacy in Location Based Services (LBSs) is vital for indoor LBSs. Fingerprinting based indoor localization method is an emerged technique in indoor localization. In such systems, Location Service Provider (LSP) may be curious and untrusted, therefore, it is better that user estimates its location by using a Partial Radio Map (PRM) that is achieved by the LSP, anonymously. In this paper, a privacy preserving method is proposed that uses Bloom filter for preserving anonymity and creating PRM during localization. In this method, the LSP cannot recognize the identity of the user by the help of the anonymizer. The proposed method has lower computational complexity compared with methods that use encryption. The proposed method also has higher accuracy in localization compared with those that use Bloom filter with one random selected AP. Then, in order to decrease the complexity and to increase the accuracy at the same time, we introduce a method that expands the radio map by authenticated users, without compromising their privacy. We also enhance the performance of this method by using Hilbert curve for

Amir Mahdi Sazdar
Cognitive Telecommunication Research Group, Department of Electrical Engineering, Shahid Beheshti University G. C., Tehran 1983963113, Iran.
E-mail: a_sazdar@sbu.ac.ir

Nasim Alikhani
Cyber Space Research Institute, Shahid Beheshti University, Tehran, Iran.

Seyed Ali Ghorashi
Cognitive Telecommunication Research Group, Department of Electrical Engineering, Shahid Beheshti University G. C., Tehran 1983963113, Iran.
Tel.: +98-21-29904135
Fax: +98-21-29902287
E-mail: a_ghorashi@sbu.ac.ir

Ahmad Khonsari
Dept. of ECE, College of Engineering, University of Tehran, Tehran 1417466191, Iran.
School of CS, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.
E-mail: a_khonsari@ut.ac.ir

preserving the ambiguity of users' location. After verifying the user's data, the LSP sends a certificate to the authenticated users. This certificate can increase the priority of users in LBS requests. In average, the proposed method has 76.93% improvement on localization results.

Keywords Privacy Preserving · Curious LSP · Partial Radio Map · Indoor Fingerprint Localization · Bloom Filter · Hilbert Curve.

1 Introduction

People need localization in indoors much more than outdoors because they spend most of their daily lives in indoors doing activities such as finding the exit and entrance in emergency operations, getting in touch with a patient in hospitals, shopping and so on [1]. GPS/GNSS based localization technologies in indoor environments have some serious failures [2], therefore, signals such as Wi-Fi, RFID, Bluetooth, and FM radio should be used for localization in such environments. One of the popular localization methods in indoor environments is fingerprinting method by using Wireless Local Area Networks (WLANs) [3,4] The fingerprinting based localization has two stages: offline stage and location estimation stage. In offline stage, measured Received Signal Strength Intensities (RSSIs) from Access Points (APs) are collected and are stored in the radio map [5]. The ***RSSI*** vector along the location coordinate is called "fingerprint" for each Reference Point (RP). Then in location estimation stage, the measured ***RSSI*** vector of Test Point (TP) is sent to Location Service Provider (LSP). The LSP estimates the user's location by pattern recognition algorithms [3,6]. One of the methods for generating the radio map is crowdsourcing method [7]. In this method, volunteers collect their ***RSSI*** vector and their locations and send them to the LSP with their smartphones. One of the challenging issues in crowdsourcing method is compromising the privacy of user by the curious LSPs or attackers.

By expanding the usage of Location Based Services (LBSs), the necessity of privacy preserving methods are growing [8,9]. Preserving the user's data, is very important for users, because if an attacker discovers the user's data (including data related to its location), the privacy of the user is endangered. Most of the localization schemes have been implemented in server-side. The privacy of user can be protected by some improvements on mechanisms of LBSs [10]. The privacy mechanisms should protect crowdsourcing-based systems against the active/passive and external/internal attacks [11]. In active attacks, the attacker often tries to change the network's data. The most common type of this attack is the attack on the service and the identity. The active attacker is an attacker who tries to use all available resources on the user-side until they are all over. However, in passive attacks the attacker has often eavesdropped the messages between users and entities from the unsecure channel. The external attacks are those attacks by individuals that are outside of the system, unlike the internal attacks that are committed by individuals in the system such as the curious LSP [11]. Privacy methods are expressed on the basis of changing

attribute-based parameters and not-changed attribute-based parameters [11]. In attribute based methods (such as methods of obfuscation and anonymization), there is no connection between user and sensed data, by changing the sensed data. In methods with not-changed attributes, the attributes or user's sensed data are protected by encryption [12,13].

There are several attempts in the literature to explain the efficiency of preserving the privacy of user's data. Authors in [14] proposed a method to preserve privacy and potential threats in Radio Frequency Identification (RFID) services by producing recommendations that help users to identify optimal service. Authors in [12] proposed a method that the LSP can partially recover true user data from perturbed data, using learning techniques such as Principal Component Analysis (PCA) and Bayes theorem, however, they did not consider the possibility that the LSP be curious. Trusted third party (TTP) as an anonymizer can preserve the identity of user from the LSP [15,16]. With expanding of computational power, and the appearance of quantum computers, the Privacy-Preserving Nearest Neighbor Query (PNNQ) is an important application of LBSs. Authors in [17] proposed a novel quantum approach to preserve the privacy of the nearest neighbor query in location-based services. In addition, this method reduced the computational costs of encryption and decryption; however, this method did not consider anonymizer to preserve the identity of user from the LSP. Authors in [18] used Hilbert curve by considering the LSP and anonymizer, however, they did not consider any anonymity scheme on user's data in fingerprinting indoor localization. Authors in [15] used another server for managing the parameters of Hilbert curve as Function Generator (FG). Also, double encryption technique [19] was used in [15] for encrypting the private information of users. This method creates the radio map with crowdsourcing method in fingerprinting indoor localization, by using Hilbert curve and double encryption technique. The parameters of Hilbert curve are managed and handled by FG between the user and the LSP; however, this method has a high computational complexity.

Existing defense mechanisms for privacy preservation in LBS are based on centralized or decentralized architecture [20]. Authors in [21] proposed a method that trusts on users and does not consider any intermediate party between users and the LSP. Also this method has high computational complexity on user-side in a decentralized manner. Authors in [13] considered a peer-peer system that the user distorts its location by a Gaussian random noise and it causes a high error in location estimating. In addition, this method does not consider the curious LSP in preserving privacy of user's data. With the development of cloud storage, the LSP usually outsources the work of managing data and localization requests to a cloud server, however, the LSP may prefer to encrypt its dataset before sending to cloud server. Cloud server in [22] should search over the encrypted dataset to answer queries. The LSP in [22] generated a key and shares it with users in the system, therefore it is possible that the LSP does not send it to all users because this method does not consider that the LSP may be curious.

There are two scenarios for localization in indoor environments, one of which preserves the privacy of user from LSP by the own user while consuming more energy and the other does not guarantee the privacy of user's location from LSP and has low power consumption [10]. The first approach is client side, in which the user sends the request to the LSP and gets the entire radio map from LSP. In this approach, no private information is sent from the user to the LSP, therefore, the computational complexity increases on the user-side and it causes more energy consumption. The second scenario is server-side in which user sends all of its private information to the LSP in order to get the responses of location requests. However, power consumption in this method is low. In this approach, the LSP may be curious or attacker, however, the accuracy of localization in this scenario is higher than that of in the former scenario. Authors in [10] proposed a method in fingerprinting indoor localization that tried to preserve the privacy of user by using Bloom filter and k-anonymity. In this method, user can estimate its location by using a PRM that was achieved from LSP, anonymously, by Bloom filter. In this method, user selects one of the APs from its measured $\boldsymbol{RSSI}$ vector, randomly, and sends the Bloom filter result of MAC address related to this AP to the LSP, and then the LSP sends a PRM to user based on this vector. Then, user can estimate its location by using this PRM. However, the localization error in this method increases, because user randomly selects one AP for computing the vector of Bloom filter. Authors in [23] proposed a method that uses Bloom filter to distribute the session keys between nodes in Wireless Sensor Networks (WSNs). This method uses Bloom filter to authenticate the communication among sensor nodes with storage efficiency. Nowadays, most of the localization methods use smartphones, and these devices have low storage capacity. Therefore, it is better to use Bloom filter for preserving the anonymity rather than using encryption schemes and do not use an encounter with challenges of key management in public key encryption methods [24].

As the usage of LBSs is expanded, replication to the user's spatial demands has become more important. Therefore, we need to take greater account of user's privacy in these systems. One of the solutions is to use public key-based encryption to keep everyone's identity unchanged. It also prevents the attacker from launching a system to respond to the user request.The method that is proposed in [25] preserves data integrity and privacy of user's location. Authors in [25] proposed a privacy preserving method in a decentralized manner, based on location proofs in outdoors. Most localization services use current user's information in order to verify the user's previous locations as a location proof. However, these methods need high-energy consumption and the computational complexity in user-side is high. Zheng et al. [26] proposed a method based on spatial-temporal location tags that uses Bloom filter in a decentralized manner. By this method, user can find out a group of users that are within its vicinity region, without revealing their locations to each other with the help of a semi-trusted LSP. However, this method does not consider anonymizer for hiding the user's identification (ID). In addition, this algorithm has high computational complexity because in this method, user uses RSA encryption

algorithm as an asymmetric encryption algorithm in private proximity testing method.

Unlike to all of the above-mentioned methods, the proposed method considers a privacy preserving method in fingerprinting indoor localization with lower computational complexity on user-side with higher accuracy in localization. It preserves the anonymity of user's data by Bloom filter that is better in terms of data storage capacity for sensors in smartphones. Further, the proposed method preserves the privacy of user's location even when there is a curious or untrusted LSP. We use anonymizer in order to preserve the ID of user from LSP. The localization error is improved by changing the use of Bloom filter compared with the algorithm in [10] in order to have lower localization error. The proposed method does not use the usual (formal) encryption algorithms; therefore, that user does not have high computational complexity and key management concern in encryption schemes. Then, we propose a method for expanding the radio map by authorized users without compromising their privacy in fingerprinting indoor localization. In this method, we use Hilbert curve for preserving the ambiguity of location of user and expanding the whole radio map. We evaluate and compare the methods proposed in [15], [26], [10] and the proposed method in terms of localization error, privacy-preserving level, computational complexity on user-side and the number of used servers. The main advantages of the proposed method are:

a) Preserving k-anonymity of user's data by using Bloom filter in location estimation stage and improving the accuracy of localization.

b) Preserving the anonymity of user's ***RSSI*** by a method that is based on the ***RSSI*** measured value of the nearest point in physical distance from PRM.

c) Using Hilbert curve for preserving the ambiguity of user's location in radio map expanding method in fingerprinting indoor localization. ion.

d) Decreasing the number of servers from three in algorithm [15] to two for the location estimation stage.

e) Giving reward and certificate for faster future localization requests, to users that are authenticated by the LSP. This certificate helps user in the further requests.

The organization of the paper is as follows. Section 2 explains some privacy preserving methods that we have compared with the proposed method. Section 3 describes the proposed method. In section 4 the simulation results and the security analysis of the proposed method are reflected. In section 5 we explain the security analysis of the proposed method. Finally, Section 6 concludes the paper.

2 Comparison of Some Privacy Preserving Methods

Privacy preserving methods are expressed on the basis of attribute-based parameters and not-changed attributes-based parameters [11]. In this section, we

review some methods in each of these two groups. As shown in Table 1, methods based on encryption methods almost have high computational complexity on user-side. Algorithms in [15] and [26] used encryption algorithms, however, it is not an efficient method when users use smartphones with low storage capacity. As shown in Table 1, location privacy algorithm in [10] used Bloom filter for preserving the anonymity of user's data by one random selected AP by user. We compare the proposed method with this method as shown in Table 1. In the proposed method, we get a balance between the cost of number of servers and the cost of computation on user-side and the accuracy of localization without compromising the privacy of user in fingerprinting indoor localization. In this paper, we propose a method in fingerprinting indoor localization that uses Bloom filter for the first AP that has maximum value on ***RSSI*** vector of user. In addition, this method uses Hilbert curve and gives signed certificate to authenticated users for their future location requests.

Table 1 A brief comparison of four methods([10,15,16,26]) with the proposed method.

Method	Approach	Computational complexity	Number of servers	Explanation	Differences with the proposed method
[10]	➢ *k*-Anonymity	➢ Bloom filter	➢ One (LSP)	➢ Using Bloom filter for preserving *k* -Anonymity	➢ The proposed method, use the first AP with maximum value on ***RSSI*** vector for creating the PRM, versus random selection of AP in [9] to increase the accuracy of localization
[15]	➢ *k*-Anonymity ➢ Ambiguity ➢ Encryption	➢ Hilbert curve, Double encryption	➢ Three (LSP, Anonymizer, FG)	➢ Using Hilbert curve for preserving ambiguity and double encryption for preserving data from eavesdroppers	➢ The proposed method, do not use any encryption algorithm and this decreases the computational complexity
[16]	➢ *k*-Anonymity ➢ Ambiguity	➢ Hilbert curve	➢ Three (LSP, Anonymizer, FG)	➢ Using FG to transfer the Hilbert curve parameters to LSP and user at each time interval	➢ The proposed method, propose an expansion radio map method without compromising the privacy of user ➢ The LSP gives certificate for authenticated users for future requests
[26]	➢ *k*-Anonymity ➢ Fuzzy extractor ➢ Encryption	➢ Bloom filter, Asymmetric encryption	➢ One (LSP)	➢ A private proximity test protocol, allowed users to test their proximity without revealing their locations ➢ Asymmetric encryption algorithm to hide user's ID	➢ The proposed method, do not use any encryption algorithm and this decreases the computational complexity

3 Proposed Method

In explaining the proposed method, we have two sections. First, we explain the proposed method for preserving the privacy of user in location estimation stage. Then, we analyze the proposed radio map expanding method by preserving the privacy of user.

3.1 Proposed Method for Preserving the Privacy of User in Location Estimation Stage

In the proposed method that preserves the privacy of user in location estimation stage, we consider two servers that work independently from each other. These servers are LSP and anonymizer. We use Bloom filter for anonymizing the AP that has maximum value on user's ***RSSI*** vector.

3.1.1 Preliminaries of Proposed Method for Preserving the Privacy of User in Location Estimation Stage

In the proposed method, we use Bloom filter in the localization process. Bloom filter is a probabilistic data structure that represents the membership of an element in a set [27]. First, an n-bit array is initialized to zero value. Then a set of k independent hash functions are used as $(h_1, h_2, ..., h_k)$. These hash functions try to avoid the collision of two messages as much as possible. Whenever there are two messages that have similar hash value, it is discovered as a collision. This filter has False Positive (FP) value. If the number of collisions are reduced, the FP value is reduced. One way for decreasing the FP is increasing the number of hash functions and increasing the size of Bloom filter. For algorithm in [10], the size of Bloom filter is equal to (1). BL is the size of Bloom filter. h is the number of hash functions. The M is the number of APs and the k is a parameter that is selected by user. User is anonymized between k-1 other users. In algorithm [10] user estimates its location by the points of PRM by pattern recognition techniques. By this method, the LSP can find out the ***RSSI*** vector of user by the maximum probability p_u.

$$BL = -\frac{h}{\ln\left(1 - \sqrt[h]{\frac{k}{M}}\right)} \tag{1}$$

3.1.2 The Proposed Method in Fingerprinting Indoor Localization by Preserving the Privacy of User

The proposed method is shown in Fig. 1. As shown in Fig. 1 we have two servers, "an anonymizer and a LSP" and both of them work independently from each other.

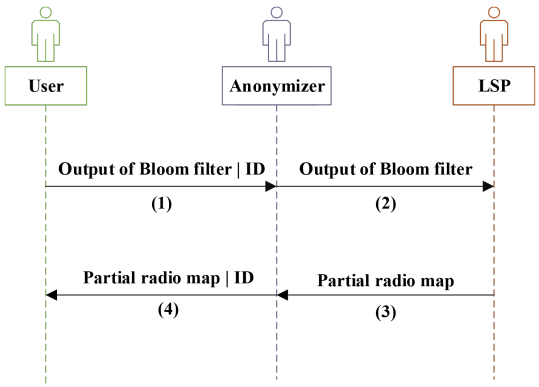

Fig. 1 The proposed method in location estimation stage.

User and LSP know the algorithms of hash functions and MAC addresses of all APs. The proposed method is composed of four follow steps:

Step 1: In this step, user selects the first AP that has maximum value on his ***RSSI*** vector and anonymizes its MAC address by using Bloom filter. Therefore it can improve the localization error compared with method represented in [10] that it localized user by one random selected AP. User sends this vector of Bloom filter to anonymizer, therefore the curios LSP cannot recognize user because anonymizer can hide the ID of user from LSP.

Step 2: Anonymizer hides the ID of user and sends the vector of Bloom filter to the LSP, and creates a table for managing the received responses from LSP for accurately giving each of them to each user.

Step 3: the LSP computes the vector of Bloom filter that can better match with vector of Bloom filter of user, in order to constructs the PRM. Then, it sends the PRM to anonymizer.

Step 4: Anonymizer sends the PRM with ID of user-to-user, and then user can estimate its location by using this PRM and its ***RSSI*** measured vector.

Proposed algorithm of preserving privacy in location estimation stage is shown in Algorithm 1. In this algorithm, the notation | is used for concatenation process. MAXR is the MAC address of AP that user $\boldsymbol{u}$ has maximum ***RSS*** value on it. $\boldsymbol{RSS}_u$ is measured ***RSSI*** vector in location of $\boldsymbol{u}$. p_u is the $\boldsymbol{u}$'s privacy probability and $f(h_1), f(h_2), f(h_3)$ are hash functions of Bloom filter. ($\mathbf{PRM}_u$) is partial radio map, (x_u, y_u) is estimated location,

Algorithm 1 Proposed Algorithm in Location Estimation Stage.

Input: $\boldsymbol{RSS}_u$, p_u, $(f(h_1), f(h_2), f(h_3))$, H_{param}
Output: Estimated location

User-side

Compute MAXR from ***RSS*** vector
$\mathbf{B}_u = createBloomFilter(\boldsymbol{RSS}_u, p_u$,MAXR)
Send $B_u|ID_u$ to anonymizer

Anonymizer-side

Send $\mathbf{B}_u$ to the LSP

LSP-side

Compute set C_u
PRM=*filter*(RM,C_u)
Send **PRM** to anonymizer

Anonymizer-side

$\mathbf{PRM}_u$=PRM $|ID_u$
Send $\mathbf{PRM}_u$ to $\boldsymbol{u}$

User-side

$(x_u, y_u) = localize(\boldsymbol{RSS}_u, \mathbf{PRM}_u)$ by NN method

3.2 Proposed Radio Mao Expansion Method by Preserving the Privacy of User

We propose a method for expanding the radio map with preserving the privacy of user. In this method, each user after estimation of its location can expand the radio map. Each user can preserve its measured ***RSSI*** vector by the help of ***RSSI*** vector of its nearest point from received PRM by (2). Measured ***RSSI*** vector in location estimation stage is valuable in indoors for enhancement of the radio map [28], because of the nature of ***RSSI*** values in indoors with varying time. First, user calculates the distance between its estimated location and the location of the nearest location in PRM as d value. User sets a threshold t_u for itself. By considering $d \leq t_u$, user anonymizes its ***RSSI*** vector by 2 (2). As shown in (2), $\boldsymbol{RSSI}_u$ is the measured ***RSSI*** of user $\boldsymbol{u}$ and $\boldsymbol{S}$ is the ***RSSI*** measured at the nearest point to user in terms of physical space. The $\mathbf{anonymized_{RSSI_u}}$ is anonymized vector of received ***RSSI*** with user $\boldsymbol{u}$.

$$\mathbf{anonymized_{RSSI_u}} \leftarrow (\mathbf{1} - \alpha)\,\mathbf{RSSI_u} + \alpha\mathbf{S} \tag{2}$$

α is a parameters that is selected by user and it is better to consider it 0.5 because by this selection, the ***RSSI*** values of test area and measurement area are considered with the same share because of dynamic nature of signals in indoors.

In this proposed radio map expansion method, there are three servers that operate independently from each other. These servers are LSP, FG, and anonymizer. FG can handle and manage the parameters of Hilbert curve at the beginning of this method among the user and the LSP. In the proposed method, each authenticated user gets a signed certificate from LSP for getting the future localization responses (such as PRM in the proposed method) faster than others.

3.2.1 Preliminaries of the Proposed Radio Map Expansion Method by Preserving the Privacy of User

In this section, we introduce the preliminaries of the proposed method. In the proposed method, we use Hilbert curve in the radio map expansion process. Hilbert Curve is an effective algorithm to obscure the location of users [15]. This curve can transfer the geographical coordinates of user in 2D to the Hilbert curve with the parameters that are associated with this curve. These parameters are curve scale factor U, order orientation of curve, starting point $((x_0, y_0))$ and Hilbert curve order that are mentioned in [15]. This transformation is similar to the encryption of geographical coordinates, however, it has lower computational complexity compared to the encryption methods. Starting point is the point at the left side of Hilbert curve that has coordinate (0,0). The transformed point $s = (x_s, y_s)$ by using Hilbert curve is equal to $< x_s, y_s >$.

$$\langle x_s, y_s \rangle = \left\lfloor \frac{(x_s, y_s) - (x_0, y_0)}{U} \right\rfloor \tag{3}$$

The coordinate of the origin of each square in this curve is (x_c, y_c), the difference between real coordinate of point s with the coordinate of region of the same square is equal to (5) [16].

$$(x_c, y_c) = U \times \langle x_s, y_s \rangle + (x_0, y_0) \tag{4}$$

$$(x_s, y_s)' = (x_s, y_s) - (x_c, y_c) \tag{5}$$

3.2.2 The Proposed Radio Map Expansion Method

The proposed method consists of five following steps:

Step 1: In this step, the user and LSP are agreed on the parameters of Hilbert curve, therefore anonymizer cannot find out the location of user because it does not know the parameters of Hilbert curve.

Step 2: User anonymizes its ***RSSI*** vector by (2). It sends "this ***RSSI*** vector, its transformed location into Hilbert curve and its ID" to anonymizer.

Step 3: Anonymizer anonymizes the ID of user sends all of other information to the LSP. Anonymizer can hide ID of user from LSP, therefore the curious LSP cannot recognize the user.

Step 4: the LSP estimates the location with the ***RSSI*** vector and compares it with received location in Hilbert curve by a threshold value. If this difference value is lower than the threshold value, the LSP stores this ***RSSI*** vector and its location in the radio map. Then, the LSP sends a signed certificate to anonymizer by its public key. This certificate authenticate this user to get faster response for future requests than others. If difference between this estimated value by the LSP and transformed location in Hilbert curve is higher than the threshold value, the LSP does not store it in radio map and does not give certificate to this user. By this method, user helps the LSP to expand the radio map without compromising the user's privacy.

Step 5: Anonymizer sends this certificate to user with its ID.

This radio map-expansion algorithm is shown in Fig. 2.

Proposed algorithm of preserving privacy in radio map expansion stage is shown in Algorithm 2. In this algorithm first the user $\boldsymbol{u}$ and the LSP must be have an agreement on parameters of Hilbert curve by help of ***FG*** and H_{param} is parameters of Hilbert curve. S is the nearest ***RSSI*** vector to the location of $\boldsymbol{u}$. The $Cert_u$ is certificate for authenticated users and C_u is the set of candidate APs that can match with B_u. The $\mathbf{anonymized_{RSSI_u}}$ is the $\mathbf{anonymized_{RSSI_u}}$ vector of $\boldsymbol{u}$.

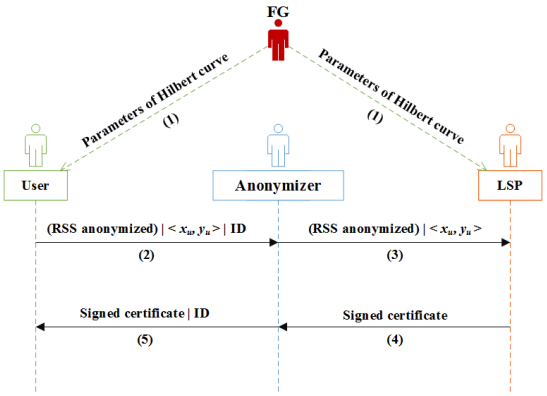

Fig. 2 Radio map expansion procedure with preserving privacy of the user.

Algorithm 2 Proposed Algorithm in Radio Map Expanding Stage.

Input: $\boldsymbol{RSS}_u$, H_{param}, α, t_u, S, $\mathbf{anonymized_{RSSI_u}}$
Output: $Cert_u$

User-side

$anonymized_{RSS_u} \leftarrow (1-\alpha)RSS_u + \alpha S$
Send $anonymized_{RSS_u}| < x_u, y_u > |ID_u$ to anonymizer

Anonymizer-side

Send $anonymized_{RSS_u}| < x_u, y_u >$ to the LSP

LSP-side

Estimate the location by $anonymized_{RSS_u}$
$LOC_{EST} = estimatedlocation_{anonymized_{RSS_u}}$
if $(| < x_u, y_u > -LOC_{EST}| \leq thershold_{value})$ **then**
    Send $Cert_u$ to anonymizer and store $< x_u, y_u > |anonymized_{RSS_u}$ in RM
end if

Anonymizer-side

Send $Cert_u|ID_u$ to $\boldsymbol{u}$

4 Simulation results

For simulation of methods, we considered four radio maps with 200, 400, 1000 and 2000 RPs and 20 TPs in each scenario, an environment with dimensions of $50m \times 50m$, in MATLAB is used. In this simulated environment, we considered that path-loss exponent value is equal to 5.9 and sigma deviation for shadowing is 8dB for all APs. We considered 100 APs. In this area, we have no wall and floor attenuation factors. We used path-loss model [4] for creating data in MATLAB. For simulations in this paper, we used 8 bits for vector of Bloom filter and three hash functions. In the proposed method and location privacy algorithm in [10], the location of user is estimated by user with NN algorithm

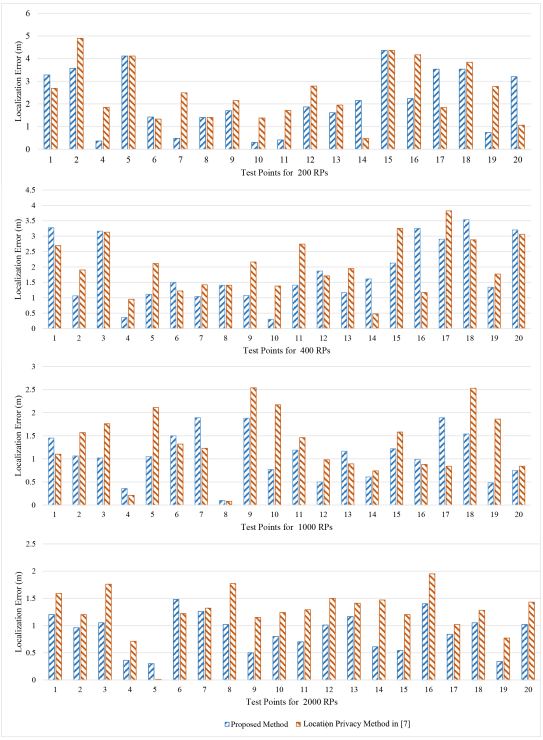

Fig. 3 The 20 TPs Localization Error Base on Meter for Different Number of RPs.

[29]. The LSP estimates the location of the user for algorithm in [15] by KNN algorithm [29] with three nearest neighbors. For showing the simulation result Fig. 3 shows the localization error by considering various number of RPs for each index of TP. Fig. 4 shows the mean localization error for location privacy algorithm in [10] and the proposed method.

Fig. 3 shows the localization error of all 20 TPs for various number of RPs. As shown in Fig. 3, by increasing the number of RPs, the error in localization may be increased for location privacy method in [10], because the selected rows by the LSP for creating the PRM did not have any relationship with the ***RSSI*** vector of user and user selected a random AP for using Bloom filter. However, the proposed method, anonymizes the AP that user has the maximum value in his ***RSSI*** vector. In the proposed method, by increasing the number of RPs the accuracy of localization is improved because the selected rows have relationship with ***RSSI*** vector of the user. Fig. 4 shows the efficiency of the proposed method compared with method in [10] when there are lower number of RPs, because it is possible to have not high number of RPs in the radio map. In average we have 76.93% improvement on localization results compared with location privacy method in [10].

The proposed method does not use any encryption despite of proposed crowdsourcing fingerprint method in [15], therefore the proposed method does

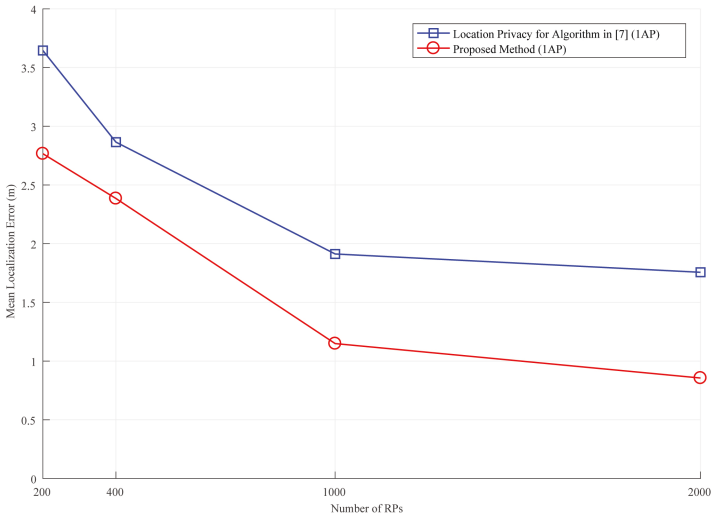

Fig. 4 Mean localization errors.

not have this high computational complexity in encryption algorithms. The localization error for the proposed method and location privacy method in [10] are estimated by user. Method represented in [15] use double encryption technique in order to give ***RSSI*** vector of user for localization and also it should manage keys of anonymizer and the LSP in public key encryption scheme. However, the proposed method and location privacy method in [10] do not use any encryption methods. Also, calculating the vector of Bloom filter is faster than any asymmetric encryption schemes in user-side. Another reason for using Bloom filter is that it has minimized the computation and storage cost to cope with the resource-constrained nature of sensors [30], and these sensors are used in smartphones. As shown in Fig. 4, the mean localization error for the proposed method is lower than the location privacy algorithm in [10] because in [10] user randomly selects AP for Bloom filter. However, we improve this selection routine to select AP with maximum $RSSI$ value to get appropriate PRM from LSP.

As Table 2 shows, the level of preserving privacy for algorithm in [10] depends on $1/k$ for anonymizing the user's data. Algorithm in [15] used three independent servers and Hilbert curve for preserving the ambiguity of user location, also we use Hilbert curve for proposed radio map expanding method. Algorithm in [26] used Bloom filter for using location tags anonymously. The proposed method uses Bloom filter for anonymizing the AP that has maximum value on user's ***RSSI*** vector in location estimation stage. All methods can preserve the privacy of user's data from both internal and external attackers. The computational complexity on user-side for the location privacy in [10] and the proposed method, are not as high as algorithms in [15] and [26]. The reason is algorithm in [15] uses double encryption schemes for ***RSSI*** vector of

user and encryption of its ID that have very high computational complexity, and also it should mange keys for public key encryption scheme. Also computational complexity of algorithm in [26] is high because in this algorithm each user encrypts its ID for proximity testing by RSA algorithm. It should be mentioned that the computational complexity is an important factor for preserving the privacy of user at the same time of the localization when user uses smartphone that has low storage space and battery life. Error of localization for algorithm in [15] is better than other examined methods, because in this method the LSP estimates the location of user and the LSP has all of the points in radio map. Therefore, error in this method is less than other reviewed algorithms. Also, the error in the proposed method is less than the method in [10] because we consider the first AP that has maximum value on user's ***RSSI*** vector for computing the vector of Bloom filter. Location privacy algorithm in [10] uses one server for localization, however, this algorithm do not have high accuracy in localization. The proposed method in location estimation stage uses two servers, and in radio map expanding method, we use three independent servers. Algorithm in [15] uses three independent servers. Algorithm in [26] should be used in a decentralized network and have compared the level of difference of distances between users for simulating the private proximity testing method. In this method, the attacker cannot manage location cheating when it was beyond the coverage of user's location tag. When the attacker passes the location based handshake algorithm, the degree of security against location cheating varies by the population density.

Table 2 shows a brief comparison of some examined methods based on the error of localization, the level of preserving privacy, the computational complexity on user-side, preserving from active attacker and the number of servers.

Table 2 A brief comparison of the proposed method with methods in [10], [15], [26].

Comparison type / Method	Number of servers	[Min ~ Max] and average localization error for 200 - 2000 RPs (*m*)
[10]	➢ *1 (LSP)*	➢ *[0.01 ~ 4.90] and 2.39*
[15]	➢ *3 (LSP, Anonymizer, FG)*	➢ *[0.01 ~ 4.12] and 2.376*
[26]	➢ *1 (LSP)*	➢ *The localization error in depends on broadcast range area of each AP and closer users for private proximity testing method in a decentralized network*
The proposed method	➢ *Two (LSP and Anonymizer) for localization and three (LSP, Anonymizer and FG) servers for expanding radio map*	➢ *[0.10 ~ 4.54] and 2.073*

5 Security Analysis of the Proposed Method

Using Bloom filter for anonymizing the AP that has the maximum element value on ***RSSI*** vector of user, makes proposed algorithm more secure with higher accuracy than method of location privacy represented in [10] because in location privacy method in [10], user selects one random AP and computes the vector of Bloom filter. In the proposed method, we use anonymizer that can

hide the ID of user from LSP. In this method, servers (LSP and anonymizer) cannot understand the real ***RSSI*** vector of user. Also the proposed method has lower computational complexity than that of method represented in [15], because for algorithms in [15] and [26] user uses double encryption technique and RSA encryption, respectively, as an asymmetric encryption method that have high computational complexity on user-side. Bloom filter is faster than asymmetric encryption schemes and it uses resources that need lower energy than asymmetric encryption algorithms. In proposed radio map expanding method, user can expand the radio map with its $\mathbf{anonymized_{RSSI_u}}$ vector and its location. It anonymizes its ***RSSI*** vector by 2 with the help of the $RSSI$ value of the nearest point to it in terms of physical distance. User uses this method versus encryption algorithm for decreasing the cost of computation and preserving its ***RSSI*** vector from eavesdroppers. The proposed method for expanding the radio map uses FG to handle the parameters of Hilbert curve between user and the LSP. In this method, authenticated users can get a certificate from the LSP to get faster responses for their future localization requests from the LSP. Table 3 shows a brief snap shot comparison of other methods with the proposed method.

Table 3 Security analysis of the proposed method and methods in [10], [15], [26].

Comparison type / Method	Level of Privacy	The Difference with the Proposed Method
[10]	➢ *Anonymity with* $1/k$	➢ *Gives appropriate PRM to user by selecting the first AP with maximum measured RSS value to increase the accuracy of localization versus randomly selecting AP in location privacy algorithm in [9]*
[15]	➢ *Anonymizer hides the ID of user from LSP* ➢ *FG preserves the location of user from anonymizer* ➢ *Double encryption preserves user's data from eavesdroppers*	➢ *Does not use any double encryption method that has higher cost of computation in compare of Bloom filter on user-side*
[26]	➢ *Using handshake and private proximity test protocol based on spatial-temporal location tags, by Bloom filter and fuzzy extractor* ➢ *Encrypting this ID of user by RSA as an asymmetric encryption algorithm*	➢ *Does not use any asymmetric encryption method that has higher cost of computation in compare of Bloom filter on user-side*
The proposed Method	➢ *Anonymity with* $1/k$ ➢ *Anonymizer hides the ID of user from LSP* ➢ *FG preserves the location of user from anonymizer*	➢ *Bloom filter for creating appropriate PRM for user and preserving k-anonymity for user's data,* ➢ *Hilbert curve for preserving the ambiguity of user's location,* ➢ *It does not use any encryption method for decreasing the cost of computation in user-side,* ➢ *It preserves the RSS vector of user from eavesdroppers by a method based on the nearest physical point to user in PRM*

6 Conclusion

By growing the needs of people in using smartphones in LBSs for almost all of their operations especially in indoors, the preserving privacy in indoors becomes an important issue. The proposed method uses Bloom filter for anonymizing the first AP that has the maximum value in user's ***RSSI*** vector in fingerprinting indoor localization. User can estimate its location without understanding its ID by the LSP because anonymizer hide the ID of user from the LSP. The proposed method make a balance between the error of localization and computational complexity when users have smartphones for localization. The proposed method improves the localization results in aver-

age up to 76.93%. Then, we proposed a method for expanding the radio map without compromising the privacy of user's data in fingerprinting indoor localization by the help of Hilbert curve. In addition, authenticated users get reward (certificate) from the LSP for getting faster responses for future requests.

Compliance with Ethical Standards

Conflict of interest: A. M. Sazdar, N. Alikhani, S. A. Ghorashi and A. Khonsari state that there are no conflicts of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Harroud, H., Ahmed, M., & Karmouch, A. (2003). Policy-driven personalized multimedia services for mobile users. IEEE Transactions on Mobile computing, 2(1), 16-24.
2. Raquet, J., & Martin, R. K. (2008). Non-GNSS radio frequency navigation. In International Conference on Acoustics, Speech and Signal Processing (ICASSP), (pp. 5308-5311).
3. El Amine, C. M., Mohamed, O., & Boualam, B. (2016). The implementation of indoor localization based on an experimental study of RSSI using a wireless sensor network. Peer-to-Peer Networking and Applications, 9(4), 795-808.
4. Alikhani, N., Amirinanloo, S., Moghtadaiee, V., & Ghorashi, S. A. (2017). Fast fingerprinting based indoor localization by Wi-Fi signals. In International Conference on Computer and Knowledge Engineering (ICCKE), (pp. 241-246).
5. Khatab, Z. E., Hajihoseini, A., & Ghorashi, S. A. (2017). A fingerprint method for indoor localization using autoencoder based deep extreme learning machine. IEEE sensors letters, 2(1), 1-4.
6. He, S., & Chan, S.-H. G. (2016). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. IEEE Communications Surveys & Tutorials, 18(1), 466-490.
7. Wang, B., Chen, Q., Yang, L. T., & Chao, H.-C. (2016). Indoor smartphone localization via fingerprint crowdsourcing: Challenges and approaches. IEEE Wireless Communications, 23(3), 82-89.
8. Wang, J., Cai, Z., Li, Y., Yang, D., Li, J., & Gao, H. (2018). Protecting query privacy with differentially private k-anonymity in location-based services. Personal and Ubiquitous Computing, 22(3), 453-469.
9. Yang, W. D., He, Y. H., Sun, L. M., Lu, X., & Li, X. (2016). An optimal query strategy for protecting location privacy in location-based services. Peer-to-Peer Networking and Applications, 9(4), 752-761.
10. Konstantinidis, A., Chatzimilioudis, G., Zeinalipour-Yazti, D., Mpeis, P., Pelekis, N., & Theodoridis, Y. (2015). Privacy-preserving indoor localization on smartphones. IEEE Transactions on Knowledge and Data Engineering, 27(11), 3042-3055.
11. Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2017). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal, 4(4), 855-869.
12. Huang, Z., Du, W., & Chen, B. (2005). Deriving private information from randomized data. In international conference on Management of data Proceedings of the ACM SIGMOD, (pp. 37-48).
13. Domingo-Ferrer, J. (2006). Microaggregation for database and location privacy. In International Workshop on Next Generation Information Technologies and Systems, (pp. 106-116).
14. Tian, Y., Song, B., & Huh, E.-N. (2011). A novel Threat Evaluation method for privacy-aware system in RFID. International Journal of Ad Hoc and Ubiquitous Computing, 8(4), 230-240.

15. Alikhani, N., Moghtadaiee, V., Sazdar, A. M., & Ghorashi, S. A. (2018). A Privacy Preserving Method for Crowdsourcing in Indoor Fingerprinting Localization. In International Conference on Computer and Knowledge Engineering (ICCKE), (pp. 58-62).
16. Peng, T., Liu, Q., & Wang, G. (2017). Enhanced location privacy preserving scheme in location-based services. IEEE Systems Journal, 11(1), 219-230.
17. Luo, Z.-y., Shi, R.-h., Xu, M., & Zhang, S. (2018). A Novel Quantum Solution to Privacy-Preserving Nearest Neighbor Query in Location-Based Services. International Journal of Theoretical Physics, 57(4), 1049-1059.
18. Khoshgozaran, A., & Shahabi, C. (2007). Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In International Symposium on Spatial and Temporal Databases, (pp. 239-257).
19. Vergara-Laurens, I. J., Mendez, D., Jaimes, L. G., & Labrador, M. (2016). A-PIE: An algorithm for preserving privacy, quality of information, and energy consumption in Participatory Sensing Systems. Pervasive and Mobile Computing, 32, 93-112.
20. Gupta, R., & Rao, U. P. (2017). An exploration to location based service and its privacy preserving techniques: a survey. Wireless Personal Communications, 96(2), 1973-2007.
21. Gupta, R., & Rao, U. P. (2017). Achieving location privacy through CAST in location based services. Journal of Communications and Networks, 19(3), 239-249.
22. Zeng, M., Zhang, K., Chen, J., & Qian, H. (2018). P3GQ: A practical privacy-preserving generic location-based services query scheme. Pervasive and Mobile Computing, 51, 56-72.
23. Qin, Z., Zhang, X., Feng, K., Zhang, Q., & Huang, J. (2014). An efficient identity-based key management scheme for wireless sensor networks using the bloom filter. Sensors, 14(10), 17937-17951.
24. Alhi, A., & Batra, S. (2016). Privacy-preserving authentication framework using bloom filter for secure vehicular communications. International Journal of Information Security (IJISP), 15(4), 433-453.
25. Wang, X., Pande, A., Zhu, J., & Mohapatra, P. (2016). STAMP: enabling privacy-preserving location proofs for mobile users. IEEE/ACM transactions on networking, 24(6), 3276-3289.
26. Zheng, Y., Li, M., Lou, W., & Hou, Y. T. (2017). Location based handshake and private proximity test with location tags. IEEE Transactions on Dependable and Secure Computing, 14(4), 406-419.
27. Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. Communications of the ACM, 13(7), 422-426.
28. He, S., Ji, B., & Chan, S.-H. G. (2016). Chameleon: Survey-free updating of a fingerprint database for indoor localization. IEEE Pervasive Computing, 15(4), 66-75.
29. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). Introduction to algorithms: MIT press.
30. Ahmadi, H., Pham, N., Ganti, R., Abdelzaher, T., Nath, S., & Han, J. (2010). Privacy-aware regression modeling of participatory sensing data. In Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, (pp. 99-112).