Dynamic Path Privacy Protection Framework for Continuous Query Service over Road Networks

Article *in* World Wide Web · August 2016

DOI: 10.1007/s11280-016-0403-3

2 authors, including:

Imran Memon
Zhejiang University
85 PUBLICATIONS **453** CITATIONS

SEE PROFILE

World Wide Web
DOI 10.1007/s11280-016-0403-3

Dynamic path privacy protection framework for continuous query service over road networks

Imran Memon[1] · **Qasim Ali Arain**[2]

Received: 14 December 2015 / Revised: 24 May 2016 / Accepted: 31 July 2016

Abstract Many applications of location based services (LBSs), it is useful or even necessary to ensure that LBSs services determine their location. For continuous queries where users report their locations periodically, attackers can infer more about users' privacy by analyzing the correlations of their query samples. The causes of path privacy problems, which emerge because the communication by different users in road network using location based services so, attacker can track continuous query information. LBSs, albeit useful and convenient, pose a serious threat to users' path privacy as they are enticed to reveal their locations to LBS providers via their queries for location-based information. Traditional path privacy solutions designed in Euclidean space can be hardly applied to road network environment because of their ignorance of network topological properties. In this paper, we proposed a novel dynamic path privacy protection scheme for continuous query service in road networks. Our scheme also conceals DPP (Dynamic Path Privacy) users' identities from adversaries; this is provided in initiator untraceability property of the scheme. We choose the different attack as our defending target because it is a particularly challenging attack that can be successfully launched without compromising any user or having access to any cryptographic keys. The security analysis shows that the model can effectively protect the user identity anonymous, location information and service content in LBSs. All simulation results confirm that our Dynamic Path Privacy scheme is not only more accurate than the related schemes, but also provide better locatable ratio where the highest it can be around 95 % of unknown nodes those can estimate their position. Furthermore, the scheme has good computation cost as well as communication and storage costs.Simulation results show that Dynamic Path Privacy has better performances compared to some related region based algorithms such as IAPIT scheme,

✉ Imran Memon
Imranmemon52@zju.edu.cn

Qasim Ali Arain
Qasim_ali_arain@yahoo.com

[1] College of Computer Science, Zhejiang University, Hangzhou, Zhejiang, China

[2] Department of Software Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan

Published online: 30 August 2016

half symmetric lens based localization algorithm (HSL) and sequential approximate maximum a posteriori (AMAP) estimator scheme.

Keywords LBSs · Localization · Range-free · Continuous query · Road network

1 Introduction

Location Based services refers to cooperate through mobile terminals and network to determine the actual location of the mobile users, provides mobile applications with location information, so can achieve various Services related to the user's Location. The existing LBS service system consists of three parts: basic user terminal, Anonymous Server and LBS Server. However, the existing research is based on the hypothesis that the anonymous device is safe and reliable, and the reliability of the anonymous apparatus at present has not been proved. Second, the LBSs awareness data within IoT (Internet of Things) space is very complicated, For example, one user's information may contain identity information, motion trail, behaviors and living habits and so on, compared with the LBSs system based on Internet, the LBSs system within IoT space is facing more serious privacy issues. To solve above problems, the researchers have put forwarded many relevant solutions. [1]. A location based services (LBSs) is an ad-hoc network consisting of a large number of LBSs services nodes deployed to sense their surrounding environment. Recently, LBSs have received a significant amount of attention academically and industrially over past few years [2]. Much of this attention may be attributed to a wide range of potential applications in several fields of interest, including military, environmental and health care [3]. In many of these applications, it is necessary for the nodes to known their own position and the position of other nodes in the networks [4]. For example, [2, 3] showed that a driver's home location can be inferred from GPS data collected on his/her vehicle even if the location data were pseudonymized or anonymized. In another study, Matsuo [4] exploited a user's indoor location data to infer a variety of personal information, such as work role, smoker or not, coffee drinker or not, and even age. For example, collecting data for emergency applications without knowing the position of LBSs services nodes is valueless. In addition, some routing protocols are built under the assumption that geographic locations of LBSs services nodes are available. This makes localization an essential middleware service in LBSs. As smartphones become increasingly popular and resource-rich, LBSs have become more feature rich and versatile, improving users' daily lives [1] by, for example, finding restaurants with their favorite menus, obtaining just-in-time coupons from nearby shopping centers, and tracking their physical fitness. For example, foursquare [15] is a popular location-based social networking application that enables users to interact with their circumstances via mobile devices. Registered users can share their location information with their friends, and receive to-do lists based on their current locations, which facilitates their exploration of exciting ongoing events in their vicinity. Another important category of applications is advertisements. For example, ShopAlerts [16], AT&T's newly launched LBS, is the first large-scale location-aware mobile marketing program in the United States, delivering coupons and special deals to registered consumers via their mobile devices when they are near a participating retailer or brand. The third commonly used LBS application is related to navigation and tracking. For example, the OnStar service provided by General Motors [17] is a comprehensive LBS system that supports a number of location-aware features such as turnby- turn navigation and stolen vehicle tracking. Other LBS

applications include location-aware weather reports and location-aware emergency medical services.

Localization privacy has been region of significant research interest. A simple solution is to equip each node with a GPS device that can provide the nodes with their accurate position. However, attaching GPS devices to all nodes in the environment may not be possible in the context of large networks because of high cost, high power consumption and environment constraint [5]. In addition, the GPS fails in indoor applications, under the ground or in dense forest [6]. The self-localization is an alternative solution of GPS, in which blind nodes (also referred to as dumb nodes, unknown nodes, or target) can estimate their location with the use of various localization algorithms. These algorithms usually share a common characteristic: most of them use a priori information about the environment such as the position (through manual pre-loading or GPS receivers) of some specific nodes, called vehicle nodes. The LBSs services nodes can also gather other information for location estimation such as the measurement of distance between two nodes, angle of signal arrival or network connectivity.

Many localization schemes have been proposed to provide location in wireless networks. On the basis of the information used for location estimation, they can be classified into two main categories: range-based and range-free. Range-based algorithms estimate the distance between nodes by using measurements such as time of arrival (ToA) [7], time difference of arrival (TDoA) [8], received signal strength indicator (RSSI) [9, 10], or angle of arrival (AoA) [11]. In the other hand range-free algorithms rely on proximity or connectivity information to estimate the node locations. Due to the hardware limitations of devices in LBS, solutions in range-free localization are being considered as a cost-effective alternative to more expensive range-based approaches. Although range-free schemes are imprecise compared with range-based schemes, they can still satisfy many application requirements and have received greater attention for localization in LBSs [12]. For example, early detection of natural disasters like wildfires and tsunamis can minimize the hazard to humans and thus minimize the risk.

1.1 Research problem

Existing LBSs system is mostly based on a central server, which is based on anonymous server and existing research is under the assumption that anonymous server itself is reliable; however, there is no authority certificate to prove the reliability of anonymous server. Once the anonymous device is attacked successfully, the user's privacy will get a serious threat. Also existing threat model intentionally simplifies the privacy protection problem by concentrating only on how to regulate the location information contained inside LBS queries. In reality, the location path privacy issue is a complicated and multifaceted problem that needs to be handled with care from several perspectives. Existing moving user's path privacy techniques in spatial-network settings largely target but short-time privacy that does not extend beyond the next road junction. Therefore, extending the anonymous server in LBS system and make it safe and reliable is our first-line work. Existing algorithms based on the k-anonymity concept [22, 24, 42], however, modify the location traces substantially and cannot meet the accuracy requirements of the traffic monitoring application. Other techniques [6, 27, 36] achieve better accuracy but cannot guarantee privacy in low user density scenarios. These path privacy protection mechanisms are based on hiding or perturbing the real locations of a user, or even

sending fake locations to the LBSs, in order to increase the uncertainty of the adversary about a user's true whereabouts. However, the evaluation of these designs usually disregards that the adversary might have some knowledge about the users' access pattern to the LBSs .Such information allows the attacker to reduce his uncertainty on the user's true location .Hence, prior evaluations overestimate the location privacy offered by a given protection system Existing area-based localization algorithms employ one of three types of primitive geometric shapes to draw the nodes' areas, namely, a triangle [11], a ring [12], and a circle [13]. The proposed scheme in [45], half symmetric lens based localization algorithm (HSL) [46] and sequential approximate maximum a posteriori (AMAP) estimator scheme [47] .Hence, it is strongly required to propose and develop a new secure and efficient path privacy protection method for Continuous Query Services in Road Networks.

1.2 Core technical contribution in the paper

To address the above problem, we propose in this paper a new region based localization algorithm, a typical range-free scheme called DPP (DYNAMIC PATH PRIVACY algorithm). The aim of DPP (DYNAMIC PATH PRIVACY) scheme is to have better performance than improve APIT scheme [45], half symmetric lens based localization algorithm (HSL) and sequential approximate maximum a posteriori (AMAP) estimator scheme [47] by using only the same parameters. Our DPP (DYNAMIC PATH PRIVACY) scheme is based on a specific geometric shape to draw the LBSs services' region. While this shape can be simply formed by using the location information of three neighboring users, DPP (DYNAMIC PATH PRIVACY) uses this information to perform a perfect test that checks whether the LBSs services is inside this shape or not. All simulation results confirm that our DPP (DYNAMIC PATH PRIVACY) scheme is not only more accurate than the related schemes, but also provide better locatable ratio where the highest it can be around 95 % of unknown nodes those can estimate their position. Furthermore, the scheme has good computation cost as well as communication and storage costs. Our proposed scheme does not require any information from neighboring LBSs services s, it uses only users' information, and so keeps computation and transmission overheads as low as possible.

1.3 Paper organization

The remainder of this paper is organized as follows: In section 2, we briefly overview some improved works of LBSs scheme. In section 3 we describe the APIT localization scheme. In section 4, we describe our proposed scheme and in section 5 we give its detailed cost analysis. In section 6, we present the simulation results. Finally, section 7 conclusion and future work.

2 Related work

By applying the personalized k-anonymity model, Gedik and Liu [13] proposed the architecture and the algorithms to protect the location privacy of the user. Chow et al. [14] proposed a distributed k-anonymity model and a peer-topeer spatial cloaking algorithm for the anonymous location based services. Ghinita et al. [15] investigated the anonymous location-based query method in the distributed mobile systems. By using the distributed hash table to select the

anonymous set of the users, Ghinita et al. [16] implemented the anonymous location-based query services in the mobile P2P system. Zhong and Hengartner [17] used the secure multiparty computation protocol to design a distributed k anonymity protocol for protecting the location privacy. By using the obfuscation method and vague location information of the user, Duckham and Kulik [18] presented a privacy-preserving location query algorithm. Mokbel [19] proposed a location-obfuscation method which allows server to record the DPP (Dynamic Path Privacy) identifier of the user but decreases the precision of the location information to protect the location privacy. By introducing the trusted third party, Mokbel et al. [20] proposed a location service query method without compromising privacy. By using the space transformation, Khoshgozaran and Shahabi [21] gave a blind evaluation of the nearest neighbor query to protect the location privacy. Ghinita et al. [22] studied the private query method in the location-based services by partitioning the space into several regions and mapping these regions into the points in Hilbert curve. Pietro and Viejo [23] developed a probabilistic and scalable protocol which guarantees the location privacy of the LBSs services s replying to the query. Raj et al. [24] proposed a realistic semi global eavesdropping attack model and showed its effectiveness in compromising an existing source-location preserving technique and designed a new protocol which preserves angle anonymity by adapting the conventional function of data mules. Zhao et al. [25] developed the optimal solutions to some special cases through dynamic programming and several heuristics for the general case to the location privacy-preserving problem. Pingley et al. [26] implemented a context-aware privacy-preserving location-based services system with integrated protection for both data privacy [52] and communication anonymity and integrated it with Google Maps. Tan [27] proposed a conditional privacy-preserving authentication and access control scheme [54] for the pervasive computing environments, in which the registration servers and authentication servers do not need to maintain any sensitive verification tables. Xi et al. [28] showed that the privacy-preserving shortest path routing problem can be solved with the private information retrieval techniques without disclosing the origin or the destination. By introducing local suppression to trajectory data anonymization to enhance the resulting data utility, Chen et al. [29] obtained a privacy model [53] on trajectory data without paying extra utility and computation cost and proposed an anonymization framework that is independent of the underlying data utility metrics and is suitable for different trajectory data mining workloads. Based on extending the private equality primitive, Buchanan et al. [30] presented a novel encryption method for preserving the location and trajectory path of a user by privacy-enhancing technologies, which has significant improvement in the computation speed. Cicek et al. [31] grouped the points of interest to create obfuscation regions around sensitive locations and used the map anonymization as a model to anonymize the trajectories and proposed a new privacy metric p-confidentiality that ensures location diversity by bounding the probability of a user visiting a sensitive location with input parameters. Li and Jung [32] proposed a fine-grained privacy-preserving location query protocol (PLQL) to solve the privacy issues in existing LBS applications and provide various location based queries. The protocol PLQL can implement semi functional encryption by novel distance computation and comparison protocol and support multilevel access control. Dewri and Thurimella [33] proposed a user-centric location based service architecture, that the users can observe the impact of location inaccuracy on the service accuracy, and Constructed a local search application and demonstrated how the meaningful information can be exchanged between the user and the service provider to allow the inference of contours depicting the change in the query results across a geographic region.

Forsgren et al. [34] Proposed Security and Trust of Public Key Cryptography Options for Host Identity Protocol to give verified identities to host using public key certification and certificate-less public key cryptography (CL-PKC). Various public key approaches for Host Identity Protocol peer authentication have been discovered. The Identity based approaches such as CL-PKC allow only PKG's to be validated, while digital signature algorithms deliver built-in key validation. Public key certificates are used, revocation lists should be checked at least every time these lists are updated. CL-PKC certificates are used to attach trust to PKG parameters, not to public user keys. In this case, revocation lists are much smaller and it is necessary to verify certificates only in Base Exchange. Seo et al. [35] solve the key escrow and key management problem, Proposed Certificate Less Hybrid Sign-Cryption without pairing operation and implemented hybrid sign-cryption scheme. Islam et al. [36] proposed secure and efficient certificate-less strong designated verifier multisignature scheme using elliptic curve cryptography (ECC) and bilinear pairings. This scheme allow to number of signatures generate common signature design verification and verified multisignature and this scheme is useful one document required to be authenticated by number of persons, applicable in several application like work flow, decision making, processes etc. Xiaoxin Wu et al. [37] certificate-less proxy re-encryption (CL-PRE) scheme for data sharing to cloud. In CL-PRE, a data owner and identified security flaws with several authentication and key establishment protocols for mobile communications, they found that the protocols do not provide authentication as intended. Liu et al. [38] presented the most important security flaws of the Self-Generated-Certificate Public Key Cryptography to captures denial of decryption attack and also provide self-generated certificate public key encryption scheme. Further, they implemented and signature and certificate scheme. Cho et al. [39] presented composite trust-based public key management (CTPKM) with no centralized trust entity with the goal of maximizing performance and fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust, using hard security approaches, as in traditional security techniques, to eliminate security vulnerabilities. Meyer et al. [40], reduce the signaling overhead and add some other security features, they proposed a new generalized approach in their paper based on asymmetric cryptography for user/network authentication and communication encryption in GSM/GPRS and UMTS with reduced signaling overhead. One exception are scientific papers published by cryptographers, that DPP (Dynamic Path Privacy)t with the weak ciphering mechanisms on the air interface of early GSM networks [41, 42], showing that the A5/1 and A5/2 ciphering algorithms are very weak and can be broken in reasonable time. With the introduction of UMTS networks, the attention has been brought to A5/3 cipher and other security mechanisms.

F. Meng et al. [43] propose an improved algorithm of APIT scheme. Its principle is as following: through APIT test, the LBSs services constructs a set of inside triangles and by dividing each triangle into three small regions it compares the strength of the received signal from vertices (users) of triangle. Then, the LBSs services finds which small region it should reside in and estimates its location as the centroid average of all the small regions obtained. However, this proposed scheme still suffers from the APIT test that can make wrong decisions. Zhang et al. [44] propose another improved algorithm of APIT scheme, called PITD (point in triangle testing based on distance) to reduce the wrong decisions made about APIT test. Its principle is as following: the LBSs services estimates distances to each vertex (user) of triangle

based on RSSI measurement to determine it coordinates by trilateration. This coordinates are used to perform the PIT testing. The test results indicate which inside triangles the LBSs services resides in. Then, the LBSs services estimates again its final position with trilateration by using the vertexes of the smallest inside triangle. However, since the LBSs services power is limited, determining the LBSs services location twice is not suitable for LBSs services [9, 55, 56]. W.Cheng et al. [45], have also proposed another improved localization algorithm for APIT that aims to reduce the wrong decisions made about APIT test. This is done through comparing RSSI values collected by neighboring outside nodes from the vertices (users) of triangle when the unknown nodes are having PIT test. The main problem of this scheme is its dependency on decisions made by neighboring nodes which can be incorrect. As we have seen in the description of the recent works cited above, the proposed algorithm cited in [44, 45] are not range-free schemes because these schemes use the absolute distances (through RSSI measurement). Therefore, comparing these schemes which are range-based schemes with APIT scheme a typical range-free scheme is not DPP (Dynamic Path Privacy) fair comparison because the result was an inevitable conclusion. In contrast, the proposed scheme in [43] does not make any assumption about the correlation between absolute distance and signal strength. For that reason, we select the proposed scheme in [45], half symmetric lens based localization algorithm (HSL) [46] and sequential approximate maximum a posteriori (AMAP) estimator scheme [47] to which we compare our work.

3 APIT localization scheme

In this section, we give a brief description of APIT localization scheme, its vulnerability due to the APIT test and the locatable node ratio which have a great impact on the performance of APIT scheme. APIT scheme divides the deployment region into nested triangular regions between beaconing nodes (users) to perform the location estimation. The presence of the LBSs services inside or outside the formed triangle regions allows a LBSs services to narrow down the region in which it can potentially reside. APIT uses the combinations of user's location and the diameter of the smallest region in which a LBSs services resides to provide good location estimation.

The LBSs services s presence inside or outside of a triangle can be checked using an APIT test. The basic idea behind APIT test is to use neighboring LBSs services s' information that contains the signal strength between a neighbor LBSs services and a given neighbor user (vertex of triangle) and through signal strength comparisons between neighboring LBSs services s, the unknown LBSs services determines whether a neighboring LBSs services is closer to a given neighboring user and thus allows this unknown LBSs services to decide whether it resides inside or outside a given triangle. The APIT depends on the number of neighboring LBSs services s that is limited, an exhaustive test on every direction is impossible. Therefore, APIT can make wrong decisions in some cases due to the irregular placement of neighbors and the edge effect. Two kinds of errors can occur: In-To-Out and Out-To-In errors. In the first kind (In-To-Out error), the test wrongly concludes that a node resides outside a triangle, whereas in practice it resides inside the triangle. In the second kind (Out-To-In error), the test wrongly concludes that a node resides inside a triangle, whereas

in practice it resides outside the triangle. Therefore, because the APIT test can fail, both the certainty of the determined LBSs services s' region and the accuracy of the estimated position are affected. Users do not trust their data over the cloud. Cloud consumers want an assurance that they can access their data whenever they want and no one else is able to get it. Moreover, authentication of users over the cloud is also an important concern to think about. APIT is a method to narrow down the localization area in which a target node resides. In APIT, the first step is APIT test, it is a way to determine an unknown node whether is inside the triangle formed. APIT test is repeated with different node combinations until all combinations are chosen. At this point, the centroid of overlap region of those triangles in which a node resides is chosen as the estimated position of unknown node. The critical step of the algorithm (APIT test) affects its localization precision. However, the incorrect decisions of APIT test are often made in APIT algorithm for uneven distribution of nodes. It judges an interior node outside the triangle (InToOut) or judges an outside one inside the triangle. When the node communication radius increases, the overlapping area will also increase. The reason why is that positions of nodes are defined by the center of mass of the polygon currently. When the polygon becomes bigger, the lower accuracy of the localization will be.

In some cases of APIT scheme, it is possible that the LBSs services nodes cannot locate themselves, and they are considered as un-localizable nodes. There are two types of these nodes.The first type is nodes that cannot construct any triangle and this is due to the limited number of user neighbors, and the second type is nodes that reside outside all possible triangular region. On the whole, highest un-localizable nodes ratio for any localization scheme negatively affects the performance of LBSs applications. With these observations, we conclude that the location accuracy and region of LBSs services are strongly affected by the wrong decision of APIT test and the ratio of localizable nodes rely on the number of nodes that reside inside a given triangular region which is limited. Therefore, we propose a new scheme that uses only the same parameters of APIT scheme which are the same varying combinations of three neighboring users and the RSSI measurements for near/far relationship in the context of the following design goals: better location accuracy and better ratio of locatable nodes compared to previous schemes.

4 Proposed algorithm

In this section, we describe our proposed algorithms. We first give the used notations, then we illustrate the basic idea of our approach, we represent the system model and we give the detailed description of the algorithms.

4.1 Privacy-preserving location based services system and algorithms

4.1.1 Anonymous location based query processing algorithm

The privacy preserving location based services system in the distributed networks includes mobile users, communication services providers CS, and location service providers LS, in which the independent trusted third party will provide the anonymous servers AS [6].

The anonymous location-based query process is as follows.

Step 1: The users acquire their locations (x, y, r) via the communication services provider, where x and y are the two dimensional location coordinates of the users, respectively, and r represents the location precision.

Step 2: The users send the service request information (U_{id}, (x, y, r), profile (A_{min}, A_{max}, K_s, k_t, t, Pre), Cont) to the anonymous server, where U_{id} is the identifier of the user, (x, y, r) is the current location information of the user, profile (A_{min}, A_{max}, K_s, k_t, t, Pre) represents the configuration file of the users, Amin and Amax denote the minimum and maximum requirements for anonymous regions, K_s and K_t are the temporal and spatial anonymous requests, respectively, t is the service time demand, Pre represents the set to the anonymity priority or services priority, and Cont is the Content of the query.

Step 3: The anonymous server receives the request from the user, generates the anonymous sets, and sends the information ((X, Y, R), (zid_1, $Cont_1$),. . , (zid_k, $Cont_k$)) to the location service server, where (X, Y, R) is the anonymous region and $zid_{필}$ is the 필th anonymous identifier of the user and $Cont_{필}$ represents the content of the ith request from the user, = 1 ~ k.

Step 4: The location service server receives the requests of the user and returns the processed results (zid_1, $result_1$),. . , (zid_k, $result_k$) to the anonymous server, and the anonymous server sends the transformed ID result to the user.

4.1.2 Select anonymous region set generation algorithm

Assume that the k users want to request location-based query services and the ith anonymous request is k_i, $k \geq \max\{k_i\}$. If the users are evenly distributed in the space range, the probability that their request information can be guessed will be $1/k$ and the probability that the actual locations of the users can be guessed will be $1/(\pi R^2)$, respectively. We know the more the users in the space range, the more the anonymous requests and the larger the generated anonymous region, the better the anonymous effect. But the computational cost to search the anonymous space will increase, and the quality of obtained location-based services may be relatively poor. The multiple searching threads are executed in parallel to accelerate the generation of the candidate anonymous set for each request queue and compute the density $p = k/(\pi R^2)$ of the user for all the candidate anonymous sets and the distribution of the users in the anonymous sets $C = |(N_1 + N_2) - (N_3 + N_4)| + |(N_1 + N_4) - (N_3 + N_2)|$, where N_j is the number of the users in the jth quadrant among the four partitioned quadrants, j = 1 ~ 4. When the location anonymous server has received the request from the user, it searches the location indexes in B-tree and inserts the location information into the request queue. If it is necessary to establish a new request queue, the location indexes will be updated. The multiple threads search in parallel and select quickly the anonymous regions in the request queues. The anonymous server handles the selected anonymous regions and provides the appropriate location services for the users. To establish the bidirectional indexes, each element in the request queues is arranged into the form (U_{id}, <x, r>, <Rmin, Rmax, K_s, t, pre>, Cont, ∗next, ∗pre). The performance

of the anonymous server is directly affected by the number of the request queues on the anonymous server. We assume that there are n location query requests and request queues on the anonymous server; the n location query requests are evenly distributed in the range with region S and the maximum anonymous radius R, and the number of the request queues is $S/(\pi R^2)$. B-tree is used to construct the location indexes with the directions X and Y on the anonymous server. The two main algorithms running on the anonymous server are the Anonymous Location Based Query Processing Algorithm and Select Anonymous Region Set Generation Algorithm, which are described as follows.

Algorithm 1. Anonymous Location Based Query Processing Algorithm.

Anonymous Location Based Query Processing Algorithm

1. **Begin**
2. The request (U_{id}, $(x,, r)$, (Rmin, Rmax, k_s , t, k_t , pre), Cont) is received and it expanded to (U_{id}, (x,y, r), (Rmin, Rmax, k_s , t, k_t , pre), Cont, A_{min}, A_{max},).
3. B-tree indexes with condition $|X - x| < 2R$max along the direction X is searched.
   - 3.1 If searching in the direction X is unsuccessful.
   - 3.2 Else request is inserted into the queue, the indexes in the direction X are updated, and the indexes in the direction Y are added.
   - 3.3 If searching in the direction X is successful, then B-tree index with condition $|Y - y| < 2R$max along the direction Y is searched.
   - 3.4 If searching in the direction Y is unsuccessful.
   - 3.5 Else current request is inserted into the request queue and the indexes in the direction Y are updated.
   - 3.6 If searching in the direction Y is successful, the current request is inserted into the request queue in the chronological order.
4. **End**

Algorithm 2. Select Anonymous Region Set Generation Algorithm.

Select Anonymous Region Set Generation Algorithm
1. **Begin**
2. The temporal-spatial queue L_T is constructed, which each element in L_T links a request queue.
3. The Request Enqueue Algorithm is executed to generate a new request queue (U_{id}, $\langle x,, r\rangle$, $\langle R_{min}, R_{max}, k_s, t, k_t,$ pre$\rangle$, Content,$*$ next, $*$pre) and this request queue is inserted into queue L_T in

4.2 Notations

For convenience, the notations used throughout the paper are given in Table 1.

4.3 Basic idea

As described in the above section, APIT scheme suffers from the wrong decision about the presence of a LBSs services inside a given triangle and this is because APIT test can fail in some cases. Therefore, our proposed scheme uses also information from three neighboring users to define a new region more reliable than inside region a given triangle used in APIT scheme. This reliability is due to the perfect test used to check the residence of LBSs services based on the node's own information not on the neighboring information as it is the case for APIT scheme.

In the following, we describe the logical way of our thinking which allowed us to define a new way to draw the LBSs services region.

Let $U_1(x_{U1}, y_{U_1})$, $U_2(x_{U2}, y_{U_2})$, and $U_3(x_{U3}, y_{U_3})$, be three neighboring users for the LBSs service with unknown position, as shown in Fig. 1.

Proposition I: (Find the closest user)

The LBSs services s is closer to at least one user U_1, U_2 or U_3. If and only if:

$$\left.\begin{array}{l} d_{s,U_1} < d_{s,U_2} \& \; d_{s,U_1} < d_{s,U_3} \\ \text{Or} \\ d_{s,U_2} < d_{s,U_1} \& \; d_{s,U_2} < d_{s,U_3} \\ \text{Or} \\ d_{s,U_3} < d_{s,U_1} \& \; d_{s,U_3} < d_{s,U_2} \end{array}\right\} \quad (1)$$

Table 1 Notations

Notation	Significance
S	LBSs services
U_m	Number of users in network
R	Communication range of each node
A	Region of the network
$\mathcal{A}$	Unknown user
N_s	Number of neighboring nodes of user
M_s	Number of neighboring node of LBSs services
L_i	Number of locatable nodes in the network
s_p	Neighboring node
(x_s, y_s)	RDPP (Dynamic Path Privacy) coordinates of LBSs services
(x_{est}, y_{est})	Estimate coordinates of LBSs services
U_i	User i
$\left(x_{U_i}, y_{U_i}\right)$	Coordinate of i^{th} user
d_{s,U_i}	The distances between LBSs services and User U_i
$d_{i,j}$	The distances between users U_i and U_j
$C_{U_i}, C_{U_j}, C_{U_k}$	Circles centered at users U_i, U_j and U_k, respectively
$RSSI_{s,U_i}$	RSSI values between LBSs services and User U_i
$RSSI_{U_i,U_j}$	RSSI values between users U_i and U_j
$RSSI_{s,s_p}$	RSSI values between LBSs services and its neighboring node s_p
NN_u	Neighboring node list of the user
NU_{lbss}	Neighboring user list of LBSs services
ACs	List of all possible combinations of three neighboring users
CMU	combine mode union
$\overline{CMU}$	Complement of combine mode union
T	Number of grid points of overlapping region
p_q	Grid point inside overlapping region
$\left(x_{p_q}, y_{p_q}\right)$	Coordinate of grid point p_q

Proposition II: ***(drawing the region)***

We suppose that user $U_1$is the closest user for s,as shown in Figure 1(a), Let draw two circles, the first one is the circle C_{U_2} centered at U_2 with radius equal to distance $d_{1,2}$ between U_2 and U_1, and the second circle is C_{U_3}centered at $U_3$with radius equal to distance $d_{1,3}$ between U_3 and U_1. If the LBSs services s is at distance to U_2 and U_3 longer than the radius of the two circles $C_{U_2}$and C_{U_3} respectively, then the LBSs services must be outside the geometric shape defined by the union of the two circles $C_{U_2}$and C_{U_3}.Thus, the actual region for LBSs services is the region of network except the region of the union of two circles $C_{U_2}$and C_{U_3}.

We delimit the actual residence region for LBSs services by drawing a third circleC_{U_1}centered at the closest user U_1 with radius equal to the longer distance between $d_{1,2}$ and $d_{1,3}$ .Figure 1(a) illustrates the final region for LBSs services by the region with green color.

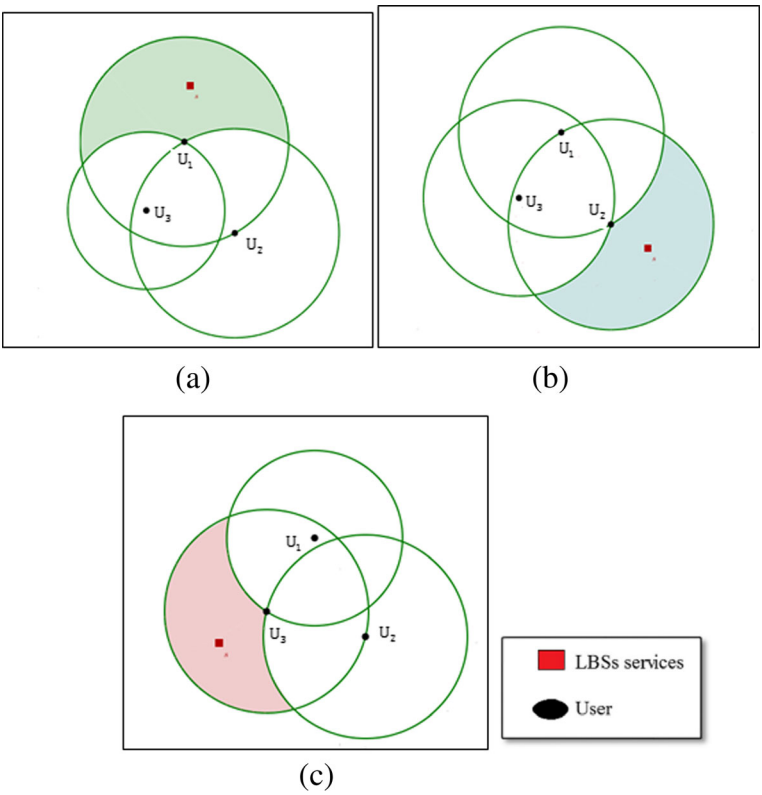


Figure 1 Illustrating the regions when: **a** U1 is the closest user to *LBSs* services, **b** U2 is the closest user to *LBSs* services, **c** U3 is the closest user to *LBSs* services

Figure 1(b) and (c) illustrate the cases when LBSs services s is closer to users U_2 and U_3, respectively .Therefore, we note that for one combination of three neighboring users ,we can get three different geometric shapes to be candidate regions for LBSs services s (green region in Figure 1(a), blue region in Figure 1(b) and red region in figure1(c)), according to the RSSI values between a LBSs services and each neighboring user . In contrast, APIT scheme can construct only one residence region for LBSs services s which is inside triangle region. We conclude that with our solution we can cover a larger region of network compared with APIT scheme and this is because the total surface region of our specific geometric shapes (union of three different geometric shapes illustrate in Figure 1) is greater than the surface region of triangle and this lead to high number of nodes that can locate themselves.

4.3.1 Exposure region for successful detection

A hostile DEV (eavesdropper) has to detect the target DEVs (victims) to enable an eavesdropping attack. Owing to the directional and adapted model, an eavesdropper can detect the existence of the victims in both its main lobe and side lobe.

Definition 1 The exposure region (ER) of a DEV is a region where the signal emitted by a DEV within this region can be detected by the DEV. The ER radius around a

receiver is the minimal distance between the receiver and a transmitter in such a way that the receiver receives the signal emitted by the transmitter successfully. If a directional is equipped on each DEV, the ER of a receiver depends on the directions of a T and an R. This includes four different cases: the T and R are inside of each other's radiation angle (Case 1), the T is inside, whereas the R is outside of each other's radiation angle (Case 2), the T is outside, whereas the R is inside of each other's radiation angle (Case 3), and the T and R are both outside each other's radiation angle (Case 4). Because an eavesdropper can detect a victim if it receives a signal emitted by the victim, a victim and an eavesdropper can be considered as a transmitter and a receiver, respectively.

Our test is guaranteed to be correct in deciding whether a LBSs services is inside the specific geometric shape defined or not. However, based on absolute distances to perform our test in LBSs does not hold well in practice. We address this issue in the next sections.

4.4 System model

This section illustrates our system model including communication and network models.

4.4.1 Communication model

APIT scheme presented in [45] uses the RSSI values comparisons between neighboring LBSs services s and neighboring users to allow an unknown node to determine whether a neighboring LBSs services is closer to /far than a given user. The validity of this assumption is tested on MICA mote, and the experiment results show that RSSI values decrease monotonically with increasing distance. Furthermore, [48, 49] confirm that is also possible to indicate near /far LBSs services s based on RSSI measurements.

As our proposed scheme DPP (DYNAMIC PATH PRIVACY) is based on the same parameters of APIT scheme, DPP (DYNAMIC PATH PRIVACY) uses also the RSSI measurements. However, instead of using the neighboring LBSs services s' information to check the closer/farther neighboring LBSs services, DPP (DYNAMIC PATH PRIVACY) is based only on the node own information where it uses the RSSI values comparisons between the unknown node itself and its neighboring users to determine the LBSs services residence region. With avoidance of neighboring LBSs services s' information, our proposed scheme does not need any communication among LBSs services s and this will reduce the communication and processing costs of our proposed scheme compared to previous schemes.

4.4.2 Network model

We consider a static location based services, so once the LBSs services s are deployed they do not leave their locations. We suppose that our network consists of a set of blind LBSs services nodes s of unknown locations and a set of user nodes $U_i$which know their absolute locations via GPS or manual pre-loading. All of these nodes are deployed randomly in a specific network region of region A. We also suppose that he communication range R of each node in the LBSs is the same.

4.5 Algorithm description

In our proposed algorithm, LBSs services s determines their location based on the beacon information transmitted by users. Initially, each LBSs services determines its region with different audible user combinations (varying combinations of three neighboring users). Once done, the LBSs services estimate its position as the Center Of Gravity (COG) of the intersection of all residence regions obtained. Our proposed algorithm involves five steps: 1) user detection, 2) Collection of localization information, 3) region formation, 4) location region refinement (or overlapping region), 5) COG calculation. In what follows, we describe all five steps in detail.

Step1: User's detection

Each user starts broadcasting a beacon message including its location information. LBSs services s and users can receive this beacon message when they are within the radio communication range of each other. Each user constructs its neighboring user list denoted by NN_u. Each raw in the NN_u includes: the user's ID, the user location (i.e. (x_{Ui}, y_{U_i})) and the RSSI corresponding to the received beacon message from the user which we denote it by $RSSI_{U_i,U_j}$. Then each user broadcasts the collected information to neighboring LBSs services s.

Step2: Collection of localization information

The LBSs services collects information from all the users that it can hear and constructs its user heard list denoted by NU_{lbss}. Each raw in the NU_{lbss} includes: the user's ID, the user location, the RSSI corresponding to beacon message received from the neighboring user which is denoted as $RSSI_{s,U_i}$ and the RSSI values of user corresponding to beacon messages received from the neighboring users is denoted as $RSSI_{U_i,U_j}$ which is obtained from NAs lists. Furthermore, the LBSs services construct another list that contains all possible combinations of three users heard. We denote it by ACs.

Step3: Region formation

After collecting neighboring users' information, the LBSs services node can determine its residence region. For three given users heard: $U_i(x_{Ui}, y_{U_i})$, $U_j\left(x_{UAj}, y_{U_j}\right)$ and U_k (x_{Uk}, y_{U_k}) ,we assume that LBSs services $s$is closer to user U_i ,if and only if :$RSSI_{s,U_i} > RSSI_{s,U_j}$ *and* $RSSI_{s,U_i} > RSSI_{s,U_k}$. Moreover, if we have: $RSSI_{s,U_j} < RSSI_{U_i,U_j}$ *and* $RSSI_{s,U_k} < RSSI_{U_i,U_k}$.Then, the LBSs services s should reside outside the geometric shape defined by the union of the two circles C_{U_j}andC_{U_k}, where $C_{U_j}$is centered at $U_j$with radius equals to distance $d_{i,j}$ between $U_j$and U_i, and circle $C_{U_k}$is centered at $U_k$with radius equals to distance $d_{i,k}$ between $U_k$and U_i. The geometric shape where the LBSs services reside is known as the complement of Combine Mode Union, which is the region of the network except the region of the union of two circles C_{U_j} and C_{U_k}. We denote it by $\overline{CMU}\left(U_j, U_k\right)$ .This initial residence region can be delimited and as the LBSs services $s$is closer to user U_i, it should be at least be inside the circle C_{U_i} centered at $U_i$with radius equals to the largest distance $d_{i,j}$or $d_{i,k}$between users U_i and $U_i$or between users $U_k$and U_i,respectively. Therefore, the final residence region will be the intersection between the region $\overline{CMU}\left(U_j, U_k\right)$ and the circle C_{U_i}.

In the following, algorithm 3 summaries the step 3.

Algorithm 3. Dynamic Path Privacy of a LBSs services.

Dynamic Path Privacy of a LBSs services
1. The Let $\mathbf{NU_{lbss}}$ be the set of neighbor users for a LBSs services.
2. Let ACs be the set of all possible three users' combinations from $\mathbf{NU_{lbss}}$ list.
3. **A** be the region of the network.
4. $R_{i,j,k}$ be the region of the LBSs services
5. **for** each **sub-set** $(\mathbf{U_j}, \mathbf{U_j}, \mathbf{U_k}) \in \mathbf{ACs}$ do
6. Let $\mathbf{U_i}$ be the nearest user **then**
7. **If** $RSSI_{s,U_j} < RSSI_{U_i,U_j}$ *and* $RSSI_{s,U_k} < RSSI_{U_i,U_k}$
8. $R_{i,j,k}=Z \setminus \overline{CMU}(U_j, U_k)$
9. $R_{i,j,k}=R_{i,j,k} \cap C_{U_i}$
10. **end if**
11. **end for**
12. **End**

Step4: Location region refinement (overlapping region)

LBSs services s can determine their final residence region based only on arithmetic operations. Since it would be computationally expensive for each LBSs services to perform the arithmetic operations, we propose to employ a grid scan algorithm that defines the overlapping region.

The grid scan algorithm has been previously used by APIT which scans each grid in the whole network region and so that it would cost too much computation time. Thus, we propose a modified grid scan algorithm which merely scans each grid in a box region within the network region.

The unknown node can receive beacon message when it is within the radio of communication range of neighboring users. So, based on the coordinates of neighboring users and the radius of communication range, we define a box region for each LBSs service, which we expect it can reside in. This box region is given by all (x, y) coordinates satisfying

$$X_{\min} - R \le x \le x_{\max} + R \;\; and \;\; y_{\min} - R \le R \le y_{\max} + R$$

Where:

x_{min} is the minimum x-coordinate value amongst all x-coordinate values of users.

y_{min} is the minimum y-coordinate value amongst all y-coordinate values of users.

x_{max} is the maximum x-coordinate value amongst all x-coordinate values of users.
y_{max} is the maximum y-coordinate value amongst all y-coordinate values of users.
R is the radius of communication range.

Our grid scan algorithm involves three steps: 1) the LBSs services places a grid of equally spaced points within its box region, as depicted in Figure 2(a). 2) For each grid point, the LBSs services holds a score in a grid score table with initial values equal to zero and for each grid point, the LBSs services performs a grid-region test to check if the grid point is included in our specific geometric shape. If the test is positive, the LBSs services increments the corresponding grid score table value by one, otherwise the value remains unchanged, as shown in Figure 2(b). This process is repeated for all the grid points.

4.5.1 Grid-region test

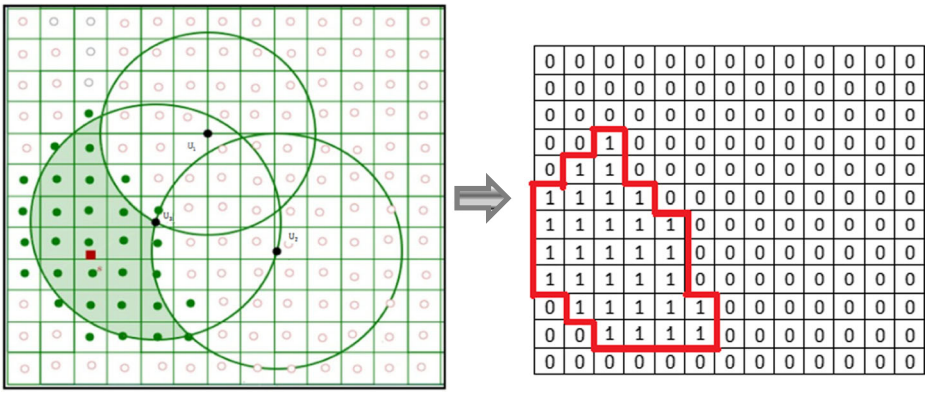
A grid point P_q is included in our specific geometric shape if it satisfies the following conditions. We assume that U_i is the closest user to LBSs services s:

$$\|P_q - U_i\| \le R \quad and \quad \|P_q - U_j\| \le R \quad and \quad \|P_q - U_k\| \le R \tag{2}$$

$$\|P_q - U_j\| \ge \|U_i - U_j\| \quad and \quad \|P_q - U_k\| \ge \|U_i - U_k\| \tag{3}$$

$$\|P_q - U_i\| \le \|U_i - U_j\| \quad \text{or} \quad \|P_q - U_i\| \le \|U_i - U_k\| \tag{4}$$

The step (2) is repeated for all possible three neighboring users' combinations. The overlapping region is defined by the grid points that have the highest score in the grid score table.



(a) (b)

Figure. 2 **a** step 3 and 4: region construction and the placement of a grid of equally-spaced points in the search region, **b** step 4: the corresponding grid score table

Step5: Location estimation

The LBSs services determine its location as the centroid of all the grid points that define the overlapping region (as shown in Figure 2(b), this region is delimited by red line):

$$(x_{est}, y_{est}) = \left(\frac{1}{T} \sum_{q=1}^{T} x_{P_q}, \frac{1}{T} \sum_{q=1}^{T} y_{P_q} \right) \tag{5}$$

Where T is the number of grid points of overlapping region, and (x_{P_q}, y_{P_q}) are coordinates of grid points.

4.6 An illustrative example of our proposed Algorithm

In this section, we present an example to further explain our proposed algorithm:

1) Each user receives beacons from its neighboring users and then constructs a Table 2 containing User ID, User location, Signal strength for each user

User U_1

2) The LBSs services receives beacons from users U_1,$U_2$and U_3, including the above Table 3 and then LBSs services constructs a table containing User ID, User location and Signal strength for each user.

Node s

3) In order to constructs its residence region, LBSs services s initially selects its closest user that has the largest signal strength between RSSI_{s,U_1}, $\mathrm{RSSI}_{s,U_2}$and RSSI_{s,U_3}. Assume it is user U_1 in this case (see Figure 3(a)). Then, it tests if it is outside the geometric shape defined by the combine mode union by executing algorithm 3 (line 7). If it is the case, the LBSs services $s$finds itself inside the green region, as depicted in Figure 3 (b) and the boundary delimitation for initial region is done by executing algorithm 3 (line 9). As depicted in Figure 3(c).

4) The LBSs services $s$repeats step 3 for varying combinations of three users by executing algorithm 1 (line 6 to 10) to determine all possible residence region for LBSs services. We note that our example demonstrates 1 combination only of three neighboring users.

Table 2 Heard users of user U_1

U_2	(x_2, y_2)	RSSI_{U_2,U_1}	RSSI_{U_2,U_3}
U_3	(x_3, y_3)	RSSI_{U_3,U_1}	RSSI_{U_3,U_2}

Table 3 Heard Users of the LBSs services

U_1	(x_1, y_1)	$RSSI_{s,U_1}$	$RSSI_{U_1,A_2}$	$RSSI_{U_1,U_3}$
U_2	(x_2, y_2)	$RSSI_{s,U_2}$	$RSSI_{U_2,U_1}$	$RSSI_{U_2,U_3}$
U_3	(x_3, y_3)	$RSSI_{s,U_3}$	$RSSI_{U_3,U_1}$	$RSSI_{U_3,U_2}$

5) The LBSs services perform the step 4 described in sections 4.4 to determine the final region of LBSs services that is the region with maximum overlap.
6) Finally, LBSs services *s*calculate its location as the center of gravity of this region.

5 Cost analysis

In this section, we evaluate the communication cost and the storage cost of our proposed scheme, and we compare theses costs with related schemes.

5.1 Communication cost

The energy efficiency is one of the most critical issues in LBSs [22]**.** A LBSs services node consumes more energy in data communication. We note that improved APIT [45], half symmetric lens based localization algorithm (HSL) [46] and sequential approximate maximum a posteriori (AMAP) estimator scheme [47] have the same communication cost, this is because existing schemes are based on APIT test which requires communications amongst nodes to maintain neighborhood state, where each user and LBSs services broadcast one message. In contrast, our proposed scheme does not require any interactions between LBSs services nodes and only users broadcast two beacon messages. The metric used to evaluate the communication cost is the number of packets sent between nodes. Therefore, APIT and improved APIT require $|M|+|N|$beacons to localize LBSs services s, while our DPP (DYNAMIC PATH PRIVACY) scheme requires $2\times|M|$ number of beacons. We notice that the three schemes

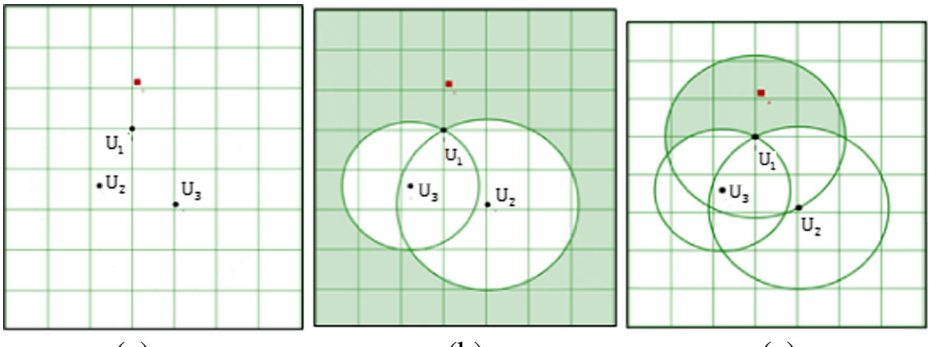


Fig. 3 Region construction

APIT [13] ,improved APIT [17] and our DPP (DYNAMIC PATH PRIVACY) schemes are classified as user based schemes which use few nodes known as references (users or beacon) for localization process. Under the assumption that the number of users is much lower than the number of LBSs services s, which means that $|M| \ll |N|$.Usually,$|M| + |N| > 2 \times |M|$. The assessment of the cost of localization depends upon the number of nodes to be localized and cost of computational complexity of the position algorithm. In DPP ,user transmission/ reception unit is attached to another user to provide communication ability with the neighboring nodes. The position estimating techniques using RSSI method to compute distance between the nodes do not require additional hardware equipment. Moreover, the additional hardware and software needed to enhance accuracy add up the cost of localization. Due to unpredictable and unreliable nature of wireless communication cost of estimating the location of user is approximated by minimizing the estimated error by iterative learning manner. Let d_{ij} be the measured distance between node i and j. Let $((x_i, y_i))$ and $((x_j, y_j))$ is the estimated coordinates of the node i and node j using the location algorithm. W estimated distance is d_{ij} and that is equated to $\sqrt{(x_i, y_i)^2 + \left(x_j, y_j\right)^2}$. The cost can be expressed as function of minimization as expressed Min (cost (i)) $= \sum_{i=1}^{N-m} \sum_{j \in M(i)} \left(d_{ij}, d_{ij}\right)^2$, Here N–M are users whose positions are to be estimated and M(i) is set of neighboring user (i). This gives the cost of estimating the position of all unknown user of the network.

We conduct that our proposed scheme DPP (DYNAMIC PATH PRIVACY) has lower number of packets and hence it has smaller communication cost than existing schemes IAPIT [45], half symmetric lens based localization algorithm (HSL) [46] and sequential approximate maximum a posteriori (AMAP) estimator scheme [47].

5.2 Storage cost

In LBS, several applications require storing data which is challenging because of the limited storage of LBSs [50]. The amount of storage required for each LBSs services node is related to the total amount of data communicated to it from neighboring nodes. Thus, we use the amount of data communicated to evaluate the storage cost of our proposed scheme and the related schemes. In the following we describe dynamic path privacy steps when the nodes require storing the data exchanged between them for the three algorithms.

In IAPIT, HSL and AMAP schemes, the node *s* receives beacons from neighboring users including (user ID, user location, RSSI between LBSs services *s* and its neighboring user) for each neighboring user and receives beacons from neighboring LBSs services s including (LBSs services ID, RSSI between the LBSs services *s* and its neighboring LBSs services) for each neighboring LBSs services. Therefore, the total storage cost of each LBSs services node in network is given by:

$$S_{\text{cost}} = ID_S + \sum_{i=1}^{\dot{M}_s} ID_{U_i} + \sum_{i=1}^{\dot{M}_s} \left(x_{U_i}, y_{U_i}\right) + \sum_{i=1}^{\dot{M}_s} RSSI_{s,U_i} + \sum_{p=1}^{\dot{N}_s} ID_{s_p} + \sum_{p=1}^{\dot{N}_s} RSSI_{s,s_p} \quad (6)$$

Where, $\dot{N}_s$ is the number of neighboring LBSs services s, ID_S is the identifier of the LBSs servicess, ID_{S_p} is the identifier of the LBSs services $s_p (p = 2, \ldots, \dot{N}_s)$, $\dot{M}_s$ is the number of

neighboring users.ID_{U_i} is the identifier of the user $U_i(i = 1, ..., M_s)$,RSSI_{s,U_i} is the RSSI between user U_i and LBSs services s.

In our proposed scheme DPP (DYNAMIC PATH PRIVACY), the LBSs services receives beacons only from neighboring users including (user ID, user location, RSSI between LBSs services $s$and its neighboring user and RSSI between neighboring users) for each user. Thus the total storage cost of our scheme is as following:

$$S'_{\mathrm{cost}} = ID_S + \sum_{i=1}^{\grave{M}_s} ID_{U_i} + \sum_{i=1}^{\grave{M}_s} (x_{U_i}, y_{U_i}) + \sum_{i=1}^{\grave{M}_s} RSSI_{S,U_i} + \sum_{i=1}^{\grave{M}_s - 1} \sum_{j=i+1}^{\grave{M}_s} RSSI_{U_i,U_j} \quad (7)$$

Where, RSSI_{U_i,U_j} is the RSSI between user U_i and user U_j $(i = 1, ..., \grave{M}_s - 1$ and $j = i + 1, ...\grave{M}_s)$.

By comparing the formula (1) and (2), and under the assumption that the number of users is much lower than the number of LBSs services s ($|M| \ll |N| \Rightarrow |M_s| \ll |N_s|$)we conduct that our scheme DPP (DYNAMIC PATH PRIVACY) use very small part of memory compared with IAPIT, HSL and AMAP schemes and thus it is suitable for location based services.

5.3 Discussion on possible attacks

In this section, to evaluate the security of the proposed scheme, we discuss the security of our proposed scheme by analyzing the following possible attacks and security properties: replay attacks, man-in-the-middle attacks, modification attacks, Denning-Sacco attacks, stolen-verifier attacks, offline dictionary attacks without the smart card, offline dictionary attacks with the smart card, session key security, known-key security, perfect forward secrecy, mutual authentication, user anonymity and biometric privacy.

5.3.1 Replay attacks

The following analysis demonstrates the proposed scheme can resist the replay attack. Suppose an adversary Bob intercepts the user *U's* previous request message *REQUEST* (*W*, *Z*) and replays it to the LBSs server to impersonate the user *U*. But, Bob cannot construct a valid $Auth_u$ and send it to the LBSs server, unless he can correctly guess $c \oplus d$ and$ST^* = h(PW) \oplus B^*$. However, Bob cannot obtain ST^* and c by decrypting the intercepted message $Z = E_{V_{cax}}(ST^* \| ID \| T \| c)$ without the knowledge of the user *U's* password *PW* and the random integer *r*, where *r* is a new integer chosen by the user *U* randomly in each session. When Bob attempts to guess *r* from *W*, he will face the elliptic curve discrete logarithm problem. In addition, without the knowledge of *c*, Bob cannot decrypt $Auth_s$ to obtain *d*. Therefore, Bob cannot generate a valid $Auth_u$ to pass the verification process of the LBSs server.

On the other hand, suppose Bob intercepts the previous *CHALLENGE* (*DPP (Dynamic Path Privacy)m*, $Auth_s$) message from the LBS server and replays it to impersonate the LBSs server. The user *U* can find out the attack by comparing the value of ST^* computed by *U* with that of the ST^* in $Auth_s$. So Bob cannot pass the verification process of the user *U* without the knowledge of user *U*'s password *PW* and biometric information B^*. In this case, no *RESPONSE* message is sent back to Bob. Therefore, the replay attack cannot succeed in the proposed scheme.

5.3.2 Man-in-the-middle attacks

Analysis shows that the proposed scheme can resist the man-in-middle attacks. In our scheme, only after mutual authentication the user U and the LBSs server can share a session key SK. Therefore, an adversary Bob cannot impersonate the user U to establish a session key with the LBSs server unless he can pass the verification process of the LBSs server. However, without the knowledge of the user U's password PW, the user U's iris template B and the random integers (c, d), Bob cannot pass verification. On the other hand, Bob cannot impersonate the LBSs server to share a session key with the user U, since he cannot correctly guess the random integer c, ST^* and SID. Thus, Bob cannot launch the man-in-middle attack to cheat either the user U or the LBSs server.

5.3.3 Modification attacks

Suppose an adversary Bob intends to impersonate the user U and modifies the $REQUEST$ message by constructing W' and Z'. Then it delivers a fraud $REQUEST$ message to the LBSs server But, Bob cannot generate a valid $W = rR = rh(PW)s^{-1}P$ without the knowledge of the secret key s. Therefore, the LBSs server can easily find this attack by decrypting the message Z and checking the ID in the identity table. Even if Bob pass this ID verification, the LBSs server can also find this attack by comparing the value of the ID in T with that of the ID in Z. In addition, Bob cannot generate a proper ST^* to pass the biometric characteristics checking without knowing the exact values. Therefore, Bob cannot impersonate the user U through fabricating the $REQUEST$ message.

Suppose an adversary Bob forges an authentication message $Auth_s$ and sends it to the user to impersonate the LBSs server. To pass the verification process of the user U, Bob needs to compute a proper ST^* and guess the correct SID and c. However, Bob cannot obtain ST^* and c by decrypting the intercepted message Z without the knowledge of the LBSs server and secret key s or the user U's password PW and the random integer r. Therefore, this attack will be found by the user U through checking the LBSs server identity SID via the smartcard. Moreover, without the knowledge of the user's password PW and biometric characteristic B^*, it is impossible to construct a proper ST^* to pass the biometric checking due to the unique feature of the user U's iris. Therefore, Bob cannot impersonate the LBSs server through fabricating the $CHALLENGE$ message.

Suppose Bob impersonates the user U and modifies the message $RESPONSE\ DPP\ (rm, Auth_u)$ sent to the LBSs server. For the same reason, if Bob cannot compute a valid ST^* and guess a correct $c \oplus d$, the LBSs server can find out that $Auth_u$ is not equivalent to its computed $h(ST^* \| c \oplus d)$. Then the LBSs server will delete SK and stop the process. Therefore, the proposed scheme can resist the modification attacks.

5.3.4 Denning-sacco attacks

Assuming an adversary Bob obtains the previous session key SK. Bob cannot obtain the U's password or the LBSs server private key s from the old session key SK. This because the session key SK is constructed by two random integers chosen by the user U and the LBSs server independently and not connected with the password or the LBSs server and private key s. Therefore, even if an old session key is compromised, the adversary Bob cannot find the user U's password PW or the LBSS server's private key s. Furthermore, in each session a fresh

session key is generated depending on the integer c and d chosen by the user U and the LBSs server respectively. Therefore, even Bob compromises an old session key, he cannot obtain other session keys since the session key$SK = h(c \oplus d)$is not connected with each other in any manner. So, the proposed scheme can resist Denning-Sacco attacks.

5.3.5 Stolen-verifier attacks

In the proposed scheme, there are no password or verification tables stored in the LBSs server database. Therefore, an adversary Bob cannot get the valuable information through DPP (Dynamic Path Privacy) sting the verification table stored on the LBSs server. So the proposed scheme can resist the stolen-verifier attacks.

5.3.6 Offline dictionary attacks without the smart card

Suppose an adversary Bob intends to carry out the offline dictionary attack. He obtains all the messages transmitting between the user U and the LBSs server through eavesdropping. In order to obtain the user's password PW, Bob needs to extract $h(PW)$ from$W = rR = rh(PW)s^{-1}P$, which is equivalent to solving an instance of elliptic curve discrete logarithm problem. Furthermore, Bob cannot obtain ST^* by decrypting the message Z without the knowledge of the user U's password PW and the random integer r or the LBSs server secret key s. Even Bob get the information ST^*, he also needs to obtain the user's iris template B^* to determine whether each of their guessed passwords is correct or not. Additionally, when Bob try to obtain the user's password PW from the information $Auth_s$, he needs to correctly guess the random integer c and the user's biometric template B^*. If Bob want to get the user's password PW from the information $Auth_u$, he needs to break the hash function, correctly guess the user U's iris template B^*. Moreover, even if Bob compromised an old session key, he could not guess the user's password PW correctly, since the session key is constructed by two random integers and not connected with the user's password PW. Therefore, the offline dictionary attack without the smart card is invalid in the proposed scheme.

5.3.7 Offline dictionary attacks with the smart card

Suppose that an adversary Bob intends to carry out the offline dictionary attack, he compromises the secret information stored in the smart card of the user U and obtains all the messages relay between the user U and the LBSs server. Compared with the offline dictionary attack without the smart card, the addition information known by Bob in this attack is the information $(R, T, h(\cdot))$ stored in the smartcard. When Bob try to extract the message $h(PW)$ form$R = h(PW)s^{-1}P$. On the other hand, Bob cannot get the message ST through decrypting the information $T = E_s(ID \| ST)$without the knowledge of the LBSs server secret key s. Moreover, even if Bob obtain the message ST, he cannot get the message $h(PW)$ to determine whether each of their guessed passwords is correct or not without the knowledge of the user's iris template B. Therefore, the offline dictionary attack with the smart card is invalid in the proposed scheme.

5.3.8 Session key security

In the proposed scheme, the session key $SK = h(c \oplus d)$is not known by anyone but only the user U and the LBSs server since the random integer c is protected by a secure symmetric

encryption algorithm throughout the authentication process. The random integer d is protected by a secure symmetric encryption algorithm and a one-way hash function during the authentication phase. In addition, the shared session key material $c \oplus d$ computed by the user U is protected by the hash function when it transmits from the user U to the LBSs server. So, none of this session key SK is known to anybody but the user U and the LBSs server . Therefore, the proposed scheme provides session key security.

5.3.9 Known-key security

In the proposed scheme, the user U and the LBSs server randomly and independently generate the random number c and d separately in each session. Therefore, the session key$SK = h(c \oplus d)$of one session is not connected with the session keys of any other sessions. So, the proposed scheme provides the known-key security.

5.3.10 Perfect forward secrecy

In the proposed scheme, the long-term private key of the user U is its password PW. Suppose that the user U's password PW is compromised by the adversary Bob, in order to get the previous session key, he needs to decrypt message Z or $Auth_s$ to obtain the random integer (c, d) or broken the one-way hash function to get $c \oplus d$. However, Bob cannot decrypt the message Z or $Auth_s$ without the knowledge of random integer r or the LBSs server secret key s. Furthermore, even if the long-term private key s of the LBSs server is also compromised, the adversary cannot figure out the previous session keys without the knowledge of hash function$h(\cdot)$. Therefore, the proposed scheme satisfies the property of perfect forward secrecy.

5.3.11 Mutual authentication

In the proposed scheme, the LBSs server and the user U can authenticate each other by checking $Auth_u$ and $Auth_s$, respectively. Therefore, the proposed scheme can provide mutual authentication.

5.3.12 User anonymity

The proposed scheme can provide user anonymity, which is demonstrated by the following proof. In the authentication phase, the user's DPP (Dynamic Path Privacy) identity is protected by a secure symmetric encryption algorithm. Therefore, even if an adversary Bob compromised the secret information stored in the smartcard and recorded the used messages transmitted between the user U and the LBSs server, he could not derive the DPP (Dynamic Path Privacy) identity of the user U without the knowledge of the user U's password PW and the random integer r or the secret key s.

5.3.13 Biometric privacy

In our scheme, the user's biometric information is protected by the hashed password while the LBSs server performs the matching algorithm. Moreover, the biometric information is also

protected by a secure symmetric encryption algorithm and hashed password when it transmits between the user U and the LBSs server. So the adversary and even the LBSs server cannot obtain the user's biometric information in the authentication process. In addition, even if the smartcard was stolen, the biometric data would not be compromised since the biometric template stored in the smartcard is protected by a secure symmetric encryption algorithm and the hashed password.

6 Simulation results

In this section, we compare the performance of our localization scheme DPP (DYNAMIC PATH PRIVACY) with other well-known range-free localization approaches improved APIT [45] which we noted by IAPIT, half symmetric lens based localization algorithm (HSL) and sequential approximate maximum a posteriori (AMAP) estimator scheme [47].We conduct simulations using NS-3 Simulator [51].

6.1 Placement model

In our simulation setting , LBSs services s and users are randomly deployed with uniform distribution within an region of size Z which is a rectangular region set at (250 m × 250 m) and at (400 m × 400 m).

6.2 System parameters

We proposed scheme DPP (DYNAMIC PATH PRIVACY) and related schemes IAPIT [45], half symmetric lens based localization algorithm (HSL) and sequential approximate maximum a posteriori (AMAP) estimator scheme [47] are an region based localization schemes, the parameters that directly affect the performance of this kind of algorithms are described as bellow:

User Node number: the total number of user nodes.
Node density: average number of nodes per node radio region
Communication radio range: the farthest distance a node radio reaches.

6.3 Evaluation

In this subsection, we evaluate the performance of localization algorithms in terms of the following metrics: localization error and the locatable ratio of nodes. We have conducted a variety of experiments to cover a wide range of system configurations including varying user nodes number and communication range for two different levels of node densities (high and low). In all of our graphs, each plotted point represents the average value of 100 trials in randomly deployed networks.

6.3.1 Localization Error

Localization error is the most significant evaluation metric in localization technologies, it is generally used as a quantitative description of localization accuracy and a lower error means better performance of localization algorithm. This error is defined as the average Euclidean

distance between the DPP (Dynamic Path Privacy) location and the estimated location of each node in the network, and then the error is computed by following formula:

$$LE = \frac{1}{N}\sum_{a\ N}\sqrt{(x-x_{est})^2 + (y-y_{est})^2} \tag{8}$$

Where, N is the set of LBSs services s, $\{(x,y)_a | a \in N\}$ is the DPP (Dynamic Path Privacy) coordinates of each LBSs services and $\{(x_{est}, y_{est})_a | a \in N\}$ is the estimated coordinates of each LBSs services.

In the evaluation, all distances including error estimation are normalized to units of node radio of communication range R to ensure generally applicable results. Then the normalized localization error is given by:

$$NLE = \frac{LE}{R} \tag{9}$$

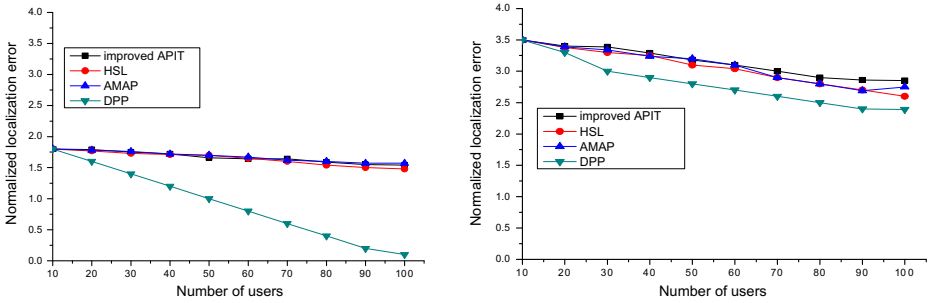
A) Localization error vs Number of users

In this experiment, we study two effects which are the number of users and node density on the localization errors. Therefore, we fix the number of nodes to 200, the communication range to 43 m, and the users number is tuned between 10 to100 with step 10. To change the node density we use two different size of the deployment region: (250 m × 250 m) and (400 m × 400 m).

Figure 4(a) and (b) show the relationship between the localization error and number of users when the network size is set to size (250 m × 250 m) and (400 m × 400 m), respectively. From these figures we can see that localization errors decrease when increasing the number of users for the four schemes represented. This can be explained by the fact that these schemes are based on the LBSs services' region. Thus, as well as the number of users increases, the probability to have successful presence test increases, and hence smaller residence regions and lower estimation error are obtained.

The curve with the label IAPIT and the curve with the label HSL, AMAP are almost the same curve. As it was discussed in the related work section, the improvement made by IAPIT is about the manner of determining the LBSs services location of HSL and AMAP schemes, which does not have a great impact on the estimation error, because IAPIT, HSL and AMAP schemes still suffer from the incorrect decision about the LBSs services region which depends on the neighbors nodes. In contrast, in our proposed scheme this is the curve with label DPP (DYNAMIC PATH PRIVACY). The estimation error is always below the both curve with label APIT and IAPIT. The accuracy of our scheme can be explained by using perfect test to check the presence of LBSs services on a location region.

It can also be observed that the localization errors of the four algorithms in Figure 4(b) are larger than that in Figure 4(a).This is due to the decreasing on the average number of neighboring LBSs services s and neighboring users per unknown node radio region from Figure 4(a) to Figure 4(b). Thus, it is clear that the localization accuracy will be influenced because four represented schemes rely on neighboring user's number to obtain an accurate region. Furthermore, IAPIT, HSL and AMAP unlike our scheme, are sensitive to the number and placement of neighboring LBSs services s which directly affects the correctness of the LBSs services presence tests.



(a) Network size (250m×250m) (b) Network size (400m×400m)

Fig. 4 Localization error Vs Number of users

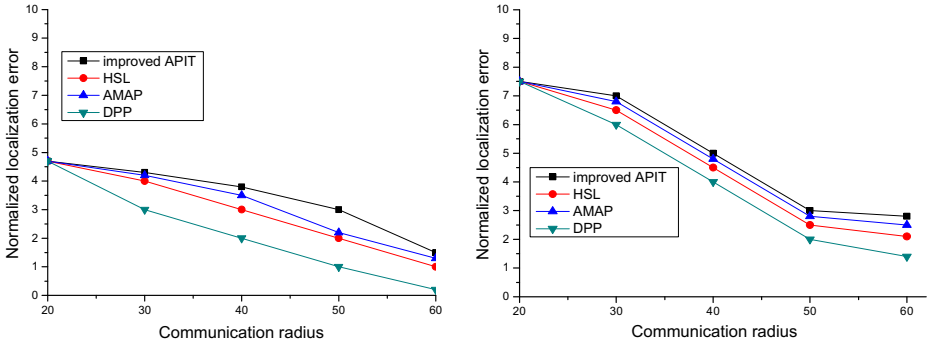
We can conclude that our proposed scheme significantly outperforms the other schemes in terms of localization accuracy. And we note that our proposed algorithm can use fewer user nodes to achieve the same localization accuracy as in IAPIT, HSL and AMAP algorithms.

B) Localization error Vs communication range

In the second experiment, we study the effect of communication range on the localization accuracy for different levels of node densities. We fix the number of user nodes to 60; the total number of unknown nodes is set as 200. The communication radius varies in the range from 20 m to 60 m with step 10, and the comparison results of the four approaches were carried out in the two levels of node density (high and low) which are shown in Figure 2.

We can clearly see in Figure 5(a) and (b) that for all three schemes represented, the localization errors are decrease with the increase of communication radius. This happens because more neighbor users participate to locate the unknown nodes as communication radius increases. Besides, the results presented in sub-section 6.3.A confirm that the localization errors decrease as the number of user's increases.

Figure 5(a) and (b) further show the effect of nodes density on the localization error. For comparison, we make similar experiments with different levels of node densities (low and high). We can see that the localization errors of the four algorithms in Figure 5(b) are greater



(a) Network size (250m×250m) (b) Network size (400m×400m)

Fig. 5 Localization error Vs communication range

than that in Figure 5 (a). This is due to the fact that when node density is low (Figure 5(b)), each node has fewer neighboring user nodes, and thus do not have enough user nodes to determine an accurate position. In addition, the impact of neighboring LBSs services s becomes greater, because IAPIT, HSL and AMAP depend on the number and placement of neighboring LBSs services s.

We can conclude that our algorithm performs better compared with the three represented algorithms in term of estimation localization error, and by increasing the communication radius of LBSs services we can reduce the required user's number.

6.3.2 Locatable ratio

The ratio of nodes that can successfully preform localization is also an important metric to evaluate the performance of localization techniques. Thus, a higher localizable ratio means better performance of localization algorithm. Here, localizable ratio is defined as the percentage of nodes can that can estimate their position. Otherwise, nodes successfully located within the residence region by localization algorithm. The locatable ratio is given by:

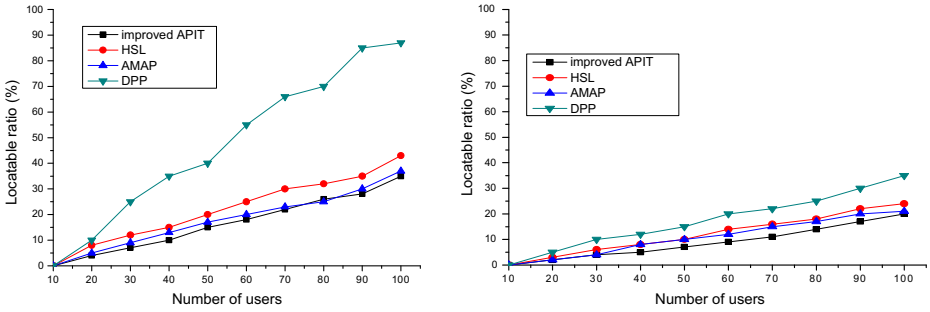
$$LR = \frac{L_i}{N} \tag{10}$$

Where, $L_i$represents the number of localizable nodes and N is the total number of nodes in network.

A) Locatable ratio Vs User percentage

Now, we investigate the impacts of the number of users and node density on the Locatable ratio. We fix the number of nodes number to 200, the range communication to 43 m, and the users number is tuned between 10 to 100 with step 10.

We can observe, in Figures 6, the two curves label IAPIT, HSL and AMAP are congruent. This happens because the proposed scheme IAPIT, HSL and AMAP does not provide any assumption to improve the number of locatable nodes in APIT. It focuses only on how to reduce the localization error. As explained in related work section, the presence test of schemes IAPIT ,HSL and AMAP can fail. Therefore, it can cause In-To-Out error which lead to low locatable ratio. However, our proposed scheme, which is the curve with label DPP (DYNAMIC PATH PRIVACY), is always above the both curves. By using the perfect test



(a) Network size (250m×250m) (b) Network size (400m×400m)

Figure 6 Locatable ratio Vs Number of users

to check the presence of LBSs services within a specific geometric shape, our scheme is characterized by its capability to contain several nodes that lead to high locatable ratio compared to IAPIT, HSL and AMAP schemes.

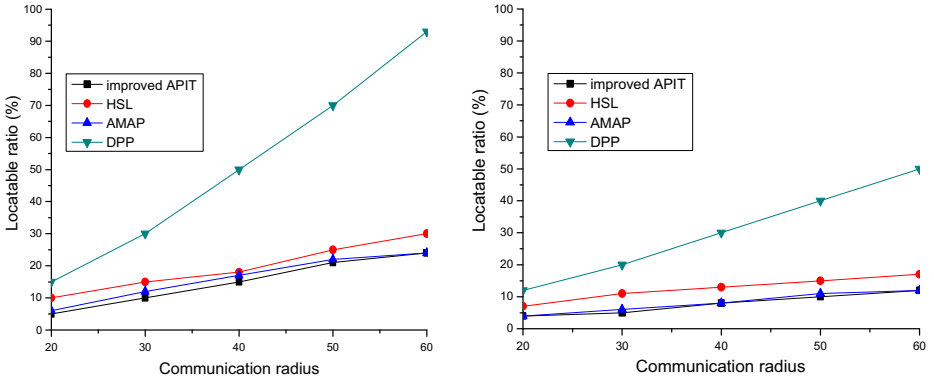
By comparing Figure 6(a) (high node density) and Figure 6 (b) (low node density), we show that locatable ratio of the four algorithms in Figure 6 (b) is lower than that in Figure 6 (a). This is because number of neighboring users and neighboring LBSs services s per unknown node decrease. Thus, the unknown nodes are relatively too far from the user nodes to hear the beacon signals, consequently, several unknown nodes fail to estimate their location.

Another reason for the poor performance of IAPIT, HSL and AMAP at low node density is that the correctness of the presence test, depends on the availability of a sufficient number of user and placement of neighboring LBSs services s, and hence the locatable ratio will be influenced. However, in our proposed scheme only the availability of neighboring users have an impact on our scheme. This is because there are no interactions between neighboring unknown nodes.

B) Locatable ratio Vs communication range

In this experiment, we study the impact of communication radius on the Locatable ratio for different node densities. We fix the number of user nodes to 60, the total number of unknown nodes is set as 200. The communication radius varies in the range of 20 m to 80 m with step 10.

Figures 7(a) and (b) show the results of experiments that test the locatable ratio with regard to communication radius. From these figures, we observe that locatable ratio of the three algorithms increases with increased communication radius of nodes. This happens because the probability of user's availability is higher with larger communication radius and thus unknown nodes find enough users to locate themselves. Furthermore, we can clearly see from Figure 7(a) and (b) that our scheme DPP (DYNAMIC PATH PRIVACY) provides better locatable ratio compared with the related schemes. There are two possible reasons for this behavior. Firstly, the wide region of the geometric shape used by our DPP (DYNAMIC PATH PRIVACY) scheme can contains several nodes compared to the inside triangle region of APIT scheme. Secondly, the fact that our DPP (DYNAMIC PATH PRIVACY) scheme, unlike IAPIT, HSL and AMAP does not need any interactions between LBSs services s for localization process. Therefore, it is



(a) Network size (250m×250m) (b) Network size (400m×400m)

Figure 7 Locatable ratio Vs communication radius

not sensitive to the density of neighboring LBSs services s which has a great impact on the correctness of the LBSs services s presence tests in IAPIT, HSL and AMAP.

Figure 7(b) presents the same experimentation with low node density. By comparing Figures 7(b) and (a), we show that the locatable ratio for low node density is lower than the locatable ratio of high node density. This is due to the fact that for low node density the number of users in the communication region of a given node is lower because the user nodes are spread over a larger region of network (400 m × 400 m). Thus several unknown nodes cannot find at least three neighboring users to locate themselves and this lead to low locatable ratio.

To summarize, all simulation results confirm that our DPP (DYNAMIC PATH PRIVACY) scheme is not only more accurate than the related schemes, but also provide better locatable ratio where the highest it can be around 95 % of unknown nodes those can estimate their position.

7 Conclusion

We proposed Dynamic Path Privacy based Localization algorithm scheme, a new distributed region based localization algorithm. Dynamic Path Privacy scheme is designed to conquer APIT scheme a typical region based algorithm. By using same parameters of APIT scheme as the same combinations number of three neighboring users and RSSI measurements for near/far relationship, DPP (DYNAMIC PATH PRIVACY) scheme outperforms IAPI, HSL and AMAPT scheme because it adopts a perfect test to identify whether the unknown node is inside the specific geometric shape formed by three neighboring users. Furthermore, for one combination of three neighboring users we can obtain three different geometric shapes instead inside triangle shape. Thus, we can cover more regions in the network and this allows several nodes to locate themselves. Also provide better locatable ratio where the highest it can be around 95 % of unknown nodes those can estimate their position. Furthermore, the scheme has good computation cost as well as communication and storage costs. Our proposed scheme does not require any information from neighboring LBSs services, it uses only users' information, and so keeps computation and transmission overheads as low as possible. Theoretical analysis and simulation results show that our proposed scheme significantly outperforms related region based schemes and improved IAPIT [45], HSL [46] and AMAP [47]. In future work, we optimized the user privacy levels over road network using genetic algorithm in term of cost, efficient privacy level, packet delay and also design optimal strategy again localization attack.

Acknowledgments We thank reviewers for their valuable comments/suggestions on the early version of the paper

References

1. Memon I.: Authentication User's Privacy: An Integrating Location Privacy Protection Algorithm for Secure Moving Objects in Location Based Services. Wirel Pers Commun. **82**(3), 1585–1600 (2015)
2. Memon I., Hussain I., Akhtar R., Chen G.: Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme. Wirel Pers Commun. **84**(2), 1487–1508 (2015)
3. Akhtar R., Leng S., Memon I., Ali M., Zhang L.: Architecture of Hybrid Mobile Social Networks for Efficient Content Delivery. Wirel Pers Commun. **80**(1), 85–96 (2015)

4. Kamenyi D.M., Wang Y., Zhang F., Memon I.: Authenticated privacy preserving for continuous query in location based services. J Comput Inf Syst. **9**(24), 9857–9864 (2013)
5. Xu J., Tang X., Hu H., Du J.: Privacy-conscious location-based queries in mobile environments. IEEE Transactions on Parallel and Distributed Systems. **21**(3), 313–326 (2010)
6. Domenic M.K., Wang Y., Zhang F., Memon I., Gustav Y.H.: Preserving users' privacy for continuous query services in road networks. In Proceedings of 2013 6th international conference on information management, innovation management and industrial engineering, ICIII 2013. **1**, 352–355 (2013)
7. Seungryeol Go, Sangdeok Kim, Jong-Wha Chong (2014).An efficient non-line-of-sight error mitigation method for TOA measurement in indoor environments.ICUIMC '14: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. Article No. 72. doi:10.1145/2557977.2558011
8. Canclini A., Bestagini P., Antonacci F., Compagnoni M., Sarti A., Tubaro S.: A robust and low-complexity source localization algorithm for asynchronous distributed microphone networks. IEEE/ACM Transactions on Audio, Speech and Language Processing (TASLP). **23**(10), 1563–1575 (2015)
9. Memon I., Mohammed M.R., Akhtar R., Memon H., Memon M.H., Shaikh R.A.: Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC). Wirel Pers Commun. **79**(1), 661–686 (2014)
10. Roberto Sadao Yokoyama, Bruno Yuji Lino Kimura, Edson dos Santos Moreira (2014). An architecture for secure positioning in a UAV swarm using RSSI-based distance estimation. SIGAPP Applied Computing Review, Volume 14 Issue 2 pp. 36-44
11. Xiuming Zhu, Pei-Chi Huang, Jianyong Meng, Song Han, Aloysius K. Mok, Deji Chen, Mark Nixon (2014). ColLoc: A collaborative location and tracking system on WirelessHART. Transactions on Embedded Computing Systems (TECS), Volume 13 Issue 4 s ACM, New York
12. Shrawan Kumar D. K. Lobiyal," (2013).An Advanced DV-Hop Localization Algorithm for Location based services". Wireless Personal Communications July 2013, Volume 71, Issue 2, pp 1365–1385
13. Gedik B., Liu L.: Protecting location privacy with personalized k-anonymity: architecture and algorithms. IEEE Trans Mob Comput. **27**(1), 1–18 (2008)
14. C.-Y. Chow, M. F. Mokbel, and X. Liu, (2006) "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems (ACM-GIS '06), pp. 171–178, Arlington, VA, USA, November 2006
15. G. Ghinita, P. Kalnis, and S. Skiadopoulos, (2007) "PRIVE: anonymous location-based queries in distributed mobile systems," in Proceedings of the 16th International World Wide Web Conference (WWW '07), pp. 371–380, Banff, Canada, May 2007.
16. Ghinita G., Kalnis P., Skiadopoulos S.: MobiHide: a mobilea peer-to-peer system for anonymous location-based queries. In: Advances in Spatial and Temporal Databases, vol. 4605 of Lecture Notes in Computer Science, pp. 221–238. Springer, Berlin, Germany (2007)
17. G. Zhong and U. Hengartner, (2009) "A distributed k-anonymity protocol for location privacy," in Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '09), pp. 1–10, Galveston, Tex, USA, March 2009.
18. M. Duckham and L. Kulik, (2005) "A formal model of obfuscation and negotiation for location privacy," in Proceedings of the 3rd International Conference on Pervasive Computing, pp. 152–170, Munich, Germany, May 2005.
19. M. F.Mokbel, (2006) "Towards privacy-aware location- based database servers," in Proceedings of the of 22nd International Conference on Data Engineering Workshops, p. 93, Atlanta, Ga, USA, April 2006.
20. M. F. Mokbel, C. Y. Chow, and W. G. Aref, (2006) "The new casper: query processing for location services without compromising privacy," in Proceedings of the of the 32nd International Conference on Very Large Data Bases, pp. 763–774, Seoul, Republic of Korea, September 2006.
21. Khoshgozaran A., Shahabi C.: Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In: Advances in Spatial and Temporal Databases, vol. 4605 of Lecture Notes in Computer Science, pp. 239–257. Springer, Berlin, Germany (2007)
22. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.- L. Tan, (2008) "Private queries in location based services: anonymizers are not necessary," in Proceedings of the ACM SIGMOD International Conference on Management of Data, pp. 121–132, Vancouver, Canada, June 2008.
23. Pietro R.D., Viejo A.: Location privacy and resilience in wireless sensor networks querying. Comput Commun. **34**(3), 515–523 (2011)
24. Raj M., Li N., Liu D., Wright M., Das S.K.: "Using data mules to preserve source location privacy in Wireless Sensor Networks," Pervasive and Mobile Computing., pp. 309–324. Springer-Verlag Berlin, Heidelberg (2012)

25. Zhao B., Wang D., Shao Z., Cao J., Su J.: Privacy aware publishing of successive location information in sensor networks. Futur Gener Comput Syst. **28**(6), 913–922 (2012)
26. Pingley A., Yu W., Zhang N., Fu X., Zhao W.: A context aware scheme for privacy-preserving location-based services. Comput Netw. **56**(11), 2551–2568 (2012)
27. Tan Z.: A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. J Netw Comput Appl. **35**(6), 1839–1846 (2012)
28. Xi Y., Schwiebert L., Shi W.: Privacy preserving shortest path routing with an application to navigation. Pervasive and Mobile Computing. **13**, 142–149 (2013)
29. Chen R., Fung B.C.M., Mohammed N., Desai B.C., Wang K.: Privacy-preserving trajectory data publishing by local suppression. Inf Sci. **231**(1), 83–97 (2013)
30. Buchanan W.J., Kwecka Z., Ekonomou E.: A privacy preserving method using privacy enhancing techniques for location based services. Mobile Networks and Applications. **18**(5), 728–737 (2013)
31. Cicek A.E., Nergiz M.E., Saygin Y.: Ensuring location diversity in privacy-preserving spatio-temporal data publishing. VLDB J. **23**(4), 609–625 (2013)
32. X. Y. Li and T. Jung, (2013) "Search me if you can: privacy- preserving location query service," in Proceedings of the 32nd IEEE International Conference on Computer Communications (IEEE INFOCOM '13), pp. 2760–2768, Turin, Italy, April 2013.
33. Dewri R., Thurimella R.: Exploiting service similarity for privacy in location-based search queries. IEEE Transactions on Parallel and Distributed Systems. **25**(2), 374–383 (2013)
34. Forsgren H., Grahn K., Karvi T., Pulkkis G.: Security and trust of public key cryptography options for HIP, In IEEE 10th international conference on computer and information technology (CIT), 2010 (pp. 1079–1084). IEEE, Bradford (2010)
35. Seo S.H., Won J., Bertino E.: POSTER: A pairing-free certificate less hybrid sign-cryption scheme for advanced metering infrastructures, In Proceedings of the 4th ACM conference on data and application security and privacy (pp. 143–146). ACM, New York (2014)
36. Islam S.H., Biswas G.: Certificateless strong designated verifier multisignature scheme using bilinear pairings, In Proceedings of the international conference on advances in computing, communications and informatics (pp. 540–546). ACM, New York (2012)
37. Wu X., Xu L., Zhang X.: Poster: A certificateless proxy re-encryption scheme for cloudbased data sharing, In Proceedings of the 18th ACM conference on computer and communications security (pp. 869–872). ACM, New York (2011)
38. Liu J.K., Au M.H., Susilo W.: Self-generated-certificate public key cryptography and Certificateless signature/encryption scheme in the standard model, In Proceedings of the 2nd ACM symposium on information, computer and communications security, (pp. 273–283). ACM, New York (2007)
39. Cho J.-H., Chan K.S., Chen I.-R.: Composite trust-based public keymanagement inmobile ad hoc networks, In Proceedings of the 28th annual ACM symposium on applied computing, (pp. 1949–1956). ACM, New York (2013)
40. Meyer U., Wetzel S.: A man-in-the-middle attack on UMTS, In Proceedings of the 3rd ACM workshop on wireless security (pp. 90–97). ACM, New York (2004)
41. Hasan M.R., Abdallah S., Raja A.: Topology aware convention emergence. In: AAMAS '14: Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems, pp. 1593–1594. International Foundation for Autonomous Agents and Multiagent Systems, Richland (2014)
42. T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, (2003) "Range-free localization schemes for large scale LBSs services networks," in Proc. ACM/IEEE MobiCom, San Diego, CA Sep. 14–19.
43. Meng F., Li X., Zhou Y.: The Improved Location Algorithm of Apit Based on Midline Segmentation for Wireless Sensor Network",. Advances in Intelligent and Soft Computing Volume. **141**, 241–248 (2012)
44. Aiqing Zhang; Xinrong Ye; Haifeng Hu Zhang, A., Ye, X., Hu, H. Point In Triangle Testing Based Trilateration Localization Algorithm In Wireless Sensor Networks", KSII Transactions on Internet & Information Systems, Oct 2012, Vol. 6 Issue 10, p2567
45. Cheng W.H., Li J., Li H.: An Improved APIT Location Algorithm for Wireless Sensor Networks". Advances in Intelligent and Soft Computing. **139,**, 113–119 (2012)
46. Noureddine Lasla, Mohamed F. Younis, Abdelraouf Ouadjaout, and Nadjib Badache (2015) An Effective Area-Based Localization Algorithm for Wireless Networks. IEEE Trans. Comput., vol. 64, no. 8, pp. 2103–2118, August 2015.
47. Zachariah D., Angelis A., Dwivedi S., Handel P.: Schedule-based sequential localization in asynchronous wireless networks. EURSIP Journal on Advances in Signal Processing. **2014**, 16 (2014)
48. Zhong Z., He T.: Rsd: A metric for achieving range-free localization beyond connectivity. IEEE Trans Parallel Distrib Syst. **22**(11), 1943–1951 (2011)
49. Bo C., Ren D., Tang S., Li X.-Y., Mao X., Huang Q., Mo L., Jiang Z., Sun Y., Liu Y., et al.: Locating sensors in the forest: A case study in greenorbs. In: INFOCOM, pp. 1026–1034. IEEE, Orlando (2012)

50. Mostafaei H.: Mohammad Shojafar, (2015) "A New Meta-heuristic Algorithm for Maximizing Lifetime of Wireless Sensor Networks ". Wirel Pers Commun. **82**(2), 723–742 (May 2015)
51. Wu X., Brown K.N., Sreenan C.J., Alvarez P., Ruffini M., Marchetti N., et al.: An XG-PON module for the NS-3 network simulator. In: SimuTools '13: Proceedings of the 6th international ICST conference on simulation tools and techniques, March 2013, pp. 195–202. ICST, Brussels (2013)
52. Muzammil M. Baig, Jiuyong Li, Jixue Liu, Xiaofeng Ding, and Hua Wang (2012).Data Privacy against Composition Attack. DASFAA (1) 2012: 320–334
53. Sun X., Li M., Wang H.: A family of enhanced (L, alpha)-diversity models for privacy preserving data publishing. Futur Gener Comput Syst. **27**(3), 348–356 (2011)
54. Wang H., Sun L., Bertino E.: Building access control policy model for privacy preserving and testing policy conflicting problems. J Comput Syst Sci. **80**(8), 1493–1503 (2014)
55. Memon I.: A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks. Wirel Pers Commun. **85**(3), 1167–1191 (2015)
56. Memon, I., Chen, L., Majid, A., Lv, M., Hussain, I., Chen, G. Travel Recommendation Using Geo-tagged Photos in Social Mediafor Tourist (2015) Wireless Personal Communications, 80 (4), pp. 1347-1362.doi:10.1007/s11277-014-2082-7