Improving The Similarity For Privacy in Location-Based Service

Reemah M. Alhebshi
Department of Computer Science
College of Computing and Information Technology. KAU
Jeddah, Saudi Arabia
ralhebshi@kau.edu.sa

Jonathan Cazalas
Department of Computer Science
College of Computing and Information Technology. KAU
Jeddah, Saudi Arabia
jcazalas@kau.edu.sa

Abstract— **With recent technological advancements in GPS-enabled devices, Location-Based Services (LBSs) have be effectively become a required commodity among users. Unfortunately, because LBS providers require users to report their location information, the issue of user privacy has become one of the foremost challenges that researchers are delving time and resources into. Most existing approaches either can't fully protect user's location privacy, or can't provide accurate LBSs. The research being conducted in this sphere is aiming to mitigate the disparity that currently prevails between the protection of user information and the accuracy of that information. In our approach to resolve this issue, we are aiming to customize a previous work of Dewri [1]. In doing so, we are proposing to increase the granularity of similarity matrix and focus the new similarity matrix in a region near to the original point. In doing so, we hope to provide enhanced accuracy of locations, while allowing location anonymity for enhanced user privacy. Moreover, it will provide the users complete control and flexibility of their system bandwidth level.**

Keywords-component; Location-Based Services (LBSs), location privacy, security, location transformation, Quality of Service (QoS), similarity matrix.

I. Introduction

Technological advancements in GPS-enabled devices, coupled with lower manufacturing costs, has resulted in smart phones effectively becoming ubiquitous. While smart phones provide a plethora of valuable applications to the user, the real power comes in their ability to leverage location-based services. *Location-Based Services* (LBSs) are permission-based applications that use real-time location intelligence from a customer's mobile device. This data facilitates the providers in rendering diversified services based off the user's geographic location and known landmarks. Therefore, having access to your location would not be of any value on its own, but relating it to other locations provide this endeavor meaning and value. To further clarify this, if a user is travelling and using such a service and they can identify points of interest along their travel path that would be of interest to them, then it would add value to the service provided. The strength of LBSs come when combining the user's geographical locations with identified points of interest (POI). As an example, a quick online search could not only enable the user to find the location of a particular POI, but combining this request with the user's geographical location can enhance the result by providing directions to said POI.

Many well-known social networking applications are experiencing an influx of usage from mobile users. This dramatic growth is estimated to increase revenues to more than € 200 million in Europe and € 450 million in America (Fig. 1). This trend is enhancing revenues to the tune of 90% in Europe, while in America the state was almost stable in 2014. Meanwhile, it is expected in 2016 to expand to more than € 400 million in Europe, whereas in America the enhancement will exceed € 500 million [3]. While the growth of Location based service brings about many new and technologically-innovative applications, there are many inherent challenges that researchers are faced with. In short, with each geotagged query sent to the backend server, the user is revealing his or her geographical location. A corrupt or malicious server can then use this user data in an attempt to infer sensitive user information. The challenge is simple: how to hide sensitive information or location data from the very server were are querying from!

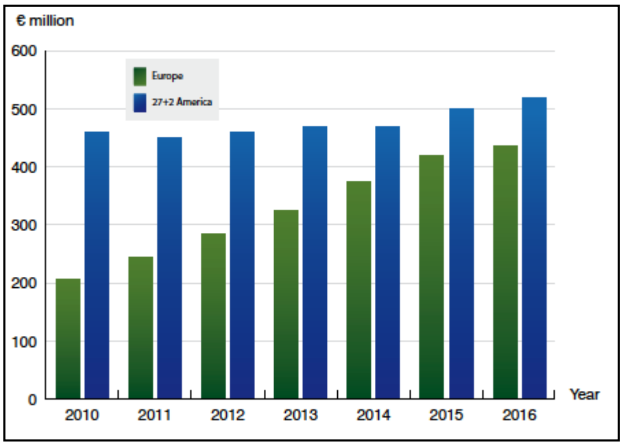


Figure 1. Mobile LBS revenue forecast. € million (2010 – 2016)

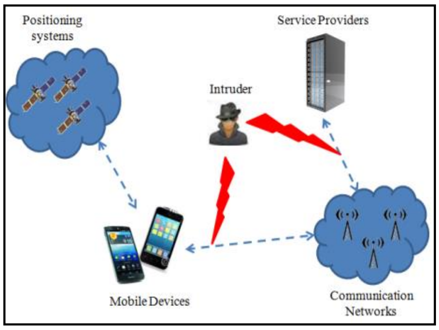


Figure 2. Location-Based Service Intruder

A. Location-Based Service and Privacy Location

While the growth of Location-based service brings about many new and technologically-innovative applications, there are many inherent challenges that researchers are faced with. Despite the fact that mapping applications are currently growing by leaps and bounds and generating the most significant revenues, inherent system limitations bottleneck advancements in location-based services and mobile mapping applications. Specifically, one major limitation is the lack of clarity in regards to what happens to a subscriber's location data. Subscriber location data can be misused by an attacker or untrusted location server, resulting in compromised privacy. Unfortunately, studies have found numerous examples of malicious attacks, wherein location data was wrongfully used for personal and economic gain [4].

Location privacy is clearly of paramount importance to users, and it is well known that there is an inverse relationship between the privacy and the efficiency of user queries. The higher level of privacy requested results in lower efficiency and accuracy of queries; on the flipside, being liberal and flexible with one's location data facilitates accuracy and efficiency. In short, there is a tradeoff and balance that must be achieved. Without surprise, there is also an alarming concern about the location data that gets collected by the service provider, and its subsequent sharing with unauthorized or untrusted parties (Fig. 2). For example; enquiring about the user's specific location will allow the user to receive accurate and efficient information. At the same time, the user loses his own privacy. In order to mitigate the privacy risks, several algorithms and novel techniques have been proposed, which prevent a service provider from getting direct access to the location data of the user.

Researchers have identified two main categories of privacy: query privacy and location privacy [5]. Query privacy refers to the privacy, or lack thereof, of the attributes of the query; location data is not considered with query privacy. Whereas, with location privacy, the concern is strictly regarding the location of the user and any possible information, which can be inferred from said location. In our approach to achieve user confidentiality, we will concentrate on location privacy.

Obfuscation has been earlier discovered through different techniques. Over the past decade, researchers injected the notion of private information retrieval into the LBS research community and proposed solutions originally focused on methods transforming user geographic location data via cryptographic techniques. User locations are hidden from the malicious nodes or attackers, and it is computationally prohibitive for attackers to identify user locations merely from the communications between the server and the user. The objective of this technique is such that the user location details are not divulged to the attackers, and it is computationally complicated for the attackers to identify user coordinates from communications between the server and nodes.

Significant efforts have been made to realize the privacy location by using dummy nodes techniques. It can characterize the dummy nodes as a service for camouflage. To clarify this meaning, suppose there is a user who wants to transfer his location to the provider's server, he will transfer his true position Pt and mix it with many false positions Pf1, Pf2, …, Pfn without any marks on the true data. These false positions are called dummies, and even if an anonymous tries to track a user, the numerous dummies confuse the anonymous by obfuscating the true position of the user. Additionally, a location *cloaking region* (CR) is used, which generates an out of sight region, effectively hiding the exact coordinates of the user. In this technique, the algorithm to process the query finds an applicant set of *Points-Of-Interest* (POI), which includes the precise results to the user.

B. Overview of Previous Work and our Limitations

There are many researchers concentrating on how to obtain the privacy and accuracy in LBSs when the user inquiries about a specific location, without any communication overload on the users bandwidth. One of the researchers was Dewri, who has a long history in the field of privacy in LBS. He has various publications relating to achieving the privacy in LBSs [6], [7], [8], [9], and [10]. His last paper [1] proposed a user-controlled privacy experience, where the user determines the desired level of privacy based on his accuracy requirements. A provider "*privacy-supportive LBS*" provides supplemental information to the user for making "*informed*" privacy decisions. The system will inform the user of the accuracy (or lack thereof) based on the privacy specifications input into the system, depending on "a service-similarity profile" which the user gets. If the user is satisfied with the result set (even if it has errors or the privacy is under the required level), they can choose to proceed with the query. If they are not satisfied, they can change the privacy level into the balance of accuracy/privacy that is acceptable to them.

The scenario of this proposal will be as follows: The user's device forwards the query to the privacy-supportive LBS. The server will respond to the user by sending a service similarity profile, which is a listing of similarity percentages based off of nearby locations. The user can then study this profile and determine if any of the locations provide enough accuracy while still providing sufficient privacy. Then the user can inform the server of his choice. Finally, the server will send the user the full query answer based on the privacy level, and accuracy, accepted by the user as described above.

Although this was a great paper that advanced the research in this area, some critical limitations have been found. This approach only has the power to "delay" disclosing one's privacy, especially if they are seeking accuracy of retrieved information. In order to achieve the goal of using low bandwidth and using a 32 × 32 km region (e.g., the metropolitan city), the similarity matrix can only have 320 × 320 grid. So, what is the problem with that? The problem is the dimension for each cell was 100 × 100 m which is a huge area. The consequence is a limited accuracy, especially in density filled geographical regions. The approach that the researchers proposed has difficulty maintaining full precision values for high-density objects. Considering that said objects are often close in proximity, most scenarios will result in small move distances, resulting in a significantly different outcome. For example, if we are only searching for shopping malls, the result of the Dewri system will result in meaningful information. On the other hand, if we are looking for a nearby taxi (very granular), cells of size mentioned above will be tremendous amounts of data, and it will not provide the accuracy requirement by the system.

Moreover, the magnitude of this matrix, which is around 124.5 KB for every requested similarity matrix, is not a large data transfer – refer to the author-. From our view, the perspective computational study will not make any crisis on the bandwidth. Unfortunately, the size of the similarity matrix, has a direct relationship with the amount of bandwidth. This creates the issue of too much bandwidth usage for/by a user, especially in cases where the user wants to limit his bandwidth (e. g. 80 KB). Thus, the similarity matrix will not be the defaulted size, but it should be actually less. On the other hand, if the user ask for more than Dewri et al size, e.g. an unlimited bandwidth, with great 4G network for every requested matrix, so the matrix will be greater than 320 × 320 grid. Conclusively, this will cover a large geographical area.

C. Contributions

We proposed Dewri supplement architecture to address these limitations by increasing the granularity of similarity matrix, and by focusing the new similarity matrix in a region near to the original query point. To enhance the high level of privacy, users don't need to send their real location to the server provider. As an alternative, they send anonymous locations. Following the motivation described in Dewri et al of giving the users a choices for a privacy level, we would like to enhance this by giving them a choice of the amount of bandwidth level they are willing to use in this application.

The goal is to develop a framework that efficiently and effectively achieves the user's privacy without surrendering the accuracy of the framework and without the requirement of providing results at such a sparse level. This system gives the user complete control and flexibility, not only in their privacy level, but also in their system bandwidth level. In general, our contributions to Dewri supplement system is to provide more accuracy and efficient results, by implementing the following:

1- Get more accuracy about the inquired location by increasing the granularity of the similarity matrix to the particular area that achieves the user satisfaction.

2- Obfuscation of the user's location by transferring the original coordinates to new anonymous locations under some condition.

3- Give the option to the user to select the amount of bandwidth.

The rest of this paper is organized as follows: Some previous works illustrating privacy-preserving location query in section II. Section III will discuss our contribution in more details. Section IV evaluates the performance of our proposed methods. Conclusions and directions for future work will be discussed in section V.

II. Related Work

Location-Based Services (LBSs) can be broadly defined as services, which are enhanced by the user of user location information. It has evolved into becoming a prevalent and imperative method to provide real-time information and direction. Many papers we reviewed are based on the various LBS systems, on their architectures, and the different governing frameworks and technologies they are built upon. The main purpose of previous papers is to understand LBS technology and to identify the central components of the system. Some papers have allowed for a concise survey of location based services, while others have looked into the technologies used for tracking the physical location of users. Some works focus on both the accuracy and reliability of LBS queries, along with the network infrastructure components used developing these valuable services.

In addition to the general idea of the LBS, the researchers discussed the impact on consumer, and utility computing offer attractive financial and technological advantages. As an example, Zhang and Mao [15] studied the effects of three individual level factors; consumption values, privacy concerns, and subjective norms on consumers' intention to adopt location-based services on their mobile phones and to spread positive word-of-mouth (WOM) about LBS. Such knowledge helps business create effective communications to attract more potential adopters. In light of the current findings, marketing communications need to heighten perceived consumption values about using LBS.

All these scientific papers give the interested reader a general idea about LBSs, and how this service was important. As mentioned previously, the inherent privacy risks in LBSs are well documented. Researchers know that while the user used one of these application services to retrieve the accuracy information, this new functionality results in a reduced level of personal privacy. Several novel schemes were proposed to facilitate a heightened level of privacy protection. Some of these papers present an overview of different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge [5], [16], [17], [18]. They clarified different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge. The aim of each paper is essentially the same: provide higher levels of privacy guarantees by revisiting this known research problem and identifying future research possibilities.

There are several works achieving privacy-preserving location queries while using a variety of methods for securing location privacy being highlighted. Privacy-preserving location has three main ideas: the idea of dummy node, the idea of cloaking-region, and the idea of encryption location. Unfortunately, several proposed methods have a problem where the quality of the LBS and Quality of Service (QoS) decreased when anonymity shows marked improvement. The next sections will cover researches on these concepts.

A. Prior Work on the Concept of Dummy Node

The main idea behind dummy nodes is to achieve k-anonymity with the usage of additional “dummy” queries. These fake queries, coupled with fake locations, simply provide “noise” and make it difficult for the LBS to identify the actual querying node. Additionally, attackers are therefore unable to use historical locations to make any claims regarding the identity of the querying node. [19]. Several techniques have been proposed, each offering the same general idea: use system generated dummy nodes to pad the real query, thereby facilitating k-anonymity among all queries. Accordingly, even if an attacker intercepts the queries, the chance of identifying the actual node would be statistically insignificant [20], [21], [22]. Pingley et al. [23] also investigated matters the usage of dummy nodes in attaining adequate privacy levels. Specifically, the focus was to prevent server correlation between query attributes and user’s location data. The authors propose a novel dummy generation algorithm, DUMMY-Q, which considers the motion vector of the user in addition to historical query attributes.

B. Prior Work on the Concept of Cloaking-Region

Cloaking regions have long been used in an effort to hide the geographical position of the querying nodes [24]. Much research has focused on the mechanisms for creating appropriately sized cloaking regions [25], [26], [27]. Miura [28] uses a hybrid concept, merging the two ideas of dummy nodes and cloaking regions, resulting in a node density-based anonymization scheme. Further, several works leverage cloaking regions by sending said regions to the location based server instead of the actual node location. Bamba et al. propose the use of l-diversity in addition to k-anonymity, thereby strengthening k-anonymity by guaranteeing that the query attributes are l-diverse among other dummy nodes [29]. Gedit et al. proposed the usage of two cloaking paradigms: spatial cloaking and temporal cloaking [30]. Queries are effectively time-stamped and separated into intervals. Related queries are merged together if they are in the same time interval. Queries are also rejected when anonymity cannot be guaranteed.

C. Prior Work on the Concept of Anonymous Location

In short, classical methods aim to encrypt user sensitive data as method of dealing with malicious attacker threats. User data is encrypted, and said data can only be decrypted by authorized individuals who possess the appropriate keys. Due to the extensive research in this area, the domain can further be subdivided into two categories: the first focuses on the actual location of the user, while the second focuses on protecting the information data of the user. [31], [32]. Of course, protecting user locations is paramount to achieving privacy, with the goal being to thwart a malicious attacker from using the user’s data to infer possible activities or even stalk the user by predicting possible future movements. Others have proposed a fine-grained query protocol, PLQP, which grants different users to have variable levels of encrypted location data. [33] Wong et al. developed an asymmetric privacy preserving mechanism, which allowed the system to preserve relative distances between points in the system. [34].

The other methodology focuses on protecting the information data of the user, which is available on the server. For example, when the user writes a note or remarks on a restaurant or any other place, this information is considered to be part of a user’s privacy. These guide researchers to search for a method to protect this privacy information [35]. Agrawal et al. suggest an encryption method called Order Preserving Encryption Scheme (OPES), which allows comparison operations to be applied directly on the encrypted data [36]. Operand decryption is still required in the computation of both SUM and AVG.

The latest two papers that discussed both methods were Dewri et al [1] and Puttaswamy et al [37]. Puttaswamy’s goal was to restrict the availability of location data from global visibility to a user’s own social circle. He introduced a novel application, LocX, which provides heightened location privacy, while not injecting uncertainty into the server results and also without reliance on security assumptions at the server level. Within his application, symmetric keys are used to both transform user locations and to encrypt all location information. Data decryption and user data querying can only be done by those possessing the correct key. Performance studies demonstrated the heightened privacy in his approach, while also fulfilling other desirable properties in terms of bandwidth, limited computation, and latency of the actual devices.

Dewri presented an innovative design for location-based service applications. His design focuses on giving the user the ability to make an informed decision by presenting privacy/utility tradeoffs to them before the user initiates a new location-based query. A user has his decision to determine the desired level of privacy according to the supplemental information coming from Privacy-supportive LBS. The privacy-supportive LBS generates a summarizing representation of the variation in the k-nearest neighbor result. This illustration of information obtained for a user as a matrix, detailing the percentage similarity of the result set with respect to the user’s current location. A cognizant conclusion dictates that the location-based service user is operating under appropriate knowledge regarding the service level implications of revealing his current location with a given and acceptable degree of impreciseness. With this understanding, the user receives, from the server, an overview of the consequence of using imprecise locations in a certain queries. Thereafter, the user query sent to the service provider is geotagged with a user-chosen location, with the goal of balancing location privacy with result accuracy. The advantage of this significant information that is exchanged between the user and the privacy-supportive is to allow the extrapolation of contours illustrating the alteration in query results over the geographic region.

III. PROPOSED TECHNIQUES

Depending on the original paper, we build our contributions to perform the results that return to the user with more accuracy with maintaining the confidentiality of user's information. While taking into account the amount of data allowed to be transferred.

Our contribution is based on three fundamental points; **First:** while Dewri's matrix measurements was 320 × 320 grid covered 32 × 32 km2, where each cell reflects to 100 × 100 m area with 124.5 KB data transferred. This measurement of each cell will not achieve the accuracy that the user is looking for, as well as providing the user with unnecessary needed information. Figure 3 demonstrated the major idea about the previous restriction. Suppose the user was in location (x, y) and his inquires was about some restaurant or coffee, Dewri's system will provide him a matrix about all the red spots, which is far from his interest. In fact, what he need is just an information about the nearest neighbor from his location. As a result, we zoom this area to attain the goal of accuracy while maintaining the same quantity of transmitted data that is described in the rectangle shape in the same figure. The new similarity matrix utilized the main concept of Dewri's matrix 320 × 320 grid - where we will still in (124.5 KB) transferred data -, but each cell assimilates to 10 × 10 m area. This new cell will achieve the accuracy and efficiency results for user.

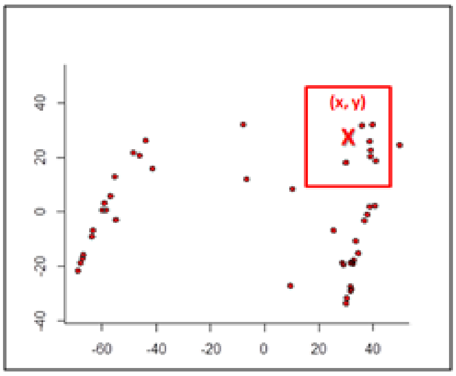


Figure 3. The New Region that the Similarity Matrix Should Covered

When the user look for a specific location around his area, the application will provide the user with the necessary information he needs. With the advent similarity matrix, the user location will be exposed, thus losing his privacy. So, the important question comes here, how we will preserve the user location? This question guided us to our **second** contribution. The answer to this question will depend on hiding the user location by making the original location anonymous (x, y) to produce a new (x`, y`). The relationship between the coordinates was exemplified in Puttaswamy [37], where he proposes a transformation of one's actual coordinate (x, y) to a fake coordinate (x`, y`) by using a private rotation degree (θ) and private shift (b). Figure 4 illustrates the idea of anonymous location for the user.

In fact, although this equation was validate in LocX application, we have some observations when applied to our advent system. This will be discussed in the coming experimental results. For leveraging the LocX equation, we made some modification to satisfy our system.

The most significant option in Dewri's system is that he gave the decision to the user to reveal his real location, where the application provides supplemental information to the user for making "informed" privacy decisions. This flexibility directs us to our **third** contribution. In this contribution, the user will be given the decision to determine his bandwidth. The greater bandwidth chosen, the greater similarity matrix is provided and vice versa.

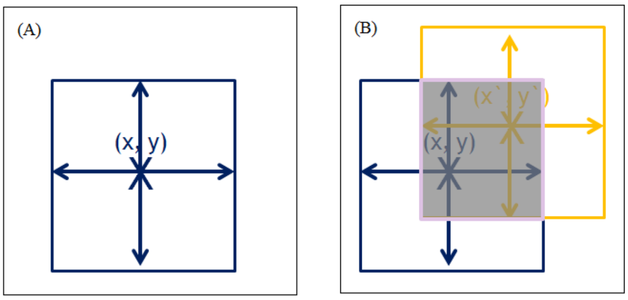


Figure 4. Anonymous User Location. (A) Clarified the Main Idea about Changing User Location. (B) The Intersection Area Between Two Regions.

IV. EXPERIMENTS RESULTS

In this section, we experimentally studied and modified the previous work to qualify the effectiveness of our changes. To prove the credibility of our equations regarding achieving system requirements, we used MATLAB to measure the distance between the user's exact location and each and every cell in the similarity matrix, thereby giving the user all available options from which to choose.

Furthermore, we generated the new similarity matrix by using the implementation provided in the *dist* and *cmdscale* functions of the R statistical package. *cmdscale* is a classical multidimensional scaling of a data matrix. In order to do the computation, it takes a set of similarities and returns to the user, a set of points such that the distances between the points are approximately equal to the similarities. *dist* refers to the computation of the distance matrix. *dist*, quite simply, computes the distance for all cells of the matrix and then returns said matrix to the user.

A. Granularity of the Similarity Matrix

A *similarity matrix* is a matrix that represents the similarity between a numbers of data points. Each cell of the similarity matrix represents a percentage similar of the query answer based off the current geographical position of the user. Suppose we have two location a = (x, y) and b = (w, z), to get the similarity between a and b, first we will inquire about the specific location for both points in a particular region. The result is a ranked list of records matching the search term from the POI database. The matched list will denote by P, where P = {P1; P2; . . . ; PN}. A ranking function R would utilize the geolocation of the user, and a top-k subset of the ranked results is sent back to him. The relationship between P and R defined as Rk (P, Pos), which specifies the result group when coupled with the actual position Pos. Thus, the result for the query is two lists Rk (a) and Rk (b).

To generate the similarity result between these two regions, we used the equation that calculates the percentage of this intersection, denoted by similarity function. It defined as follows:

$$Sim\ [a,\, b] = \left| \frac{Rk\ (P,a) \cap Rk\ (P,b)}{k} \right| \times 100$$

Figure 5 explain the main idea of how similarity function works. It is the dark shadow in the intersection between the two regions represented. The numbers presented found in this intersection symbolize the result of Sim function for shown regions. To simplify the concept, a given example follows:

The user 1 and user 2 inquire a ranked list P for top-10 nearest neighbor, in the position (x, y), (w, z) respectively. The results will be as followed:

Puser1 = {1,2,3,4,5,6,7,8,9,10}
Puser2 = {1,2,3,4,5,6,7,8}, thus:

$$Sim\ [user1,\, user2] = \left| \frac{3}{10} \right| \times 100 = 30\ \%$$

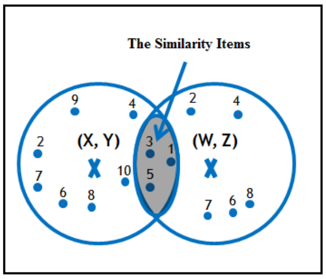


Figure 5. The Similarity items between two Regions Overlap.

Suppose Sx,y is a matrix of r rows and c columns, for every cell of matrix it signified the similarity function between user position (x, y) and the position in the matrix (i, j). It defined as followed:

$$Sx,y\ [i,\, j] = Sim\ \{(x,\, y),\, (i,\, j)\}$$

For example, if we look at a number in cell [54, 123], what does the number in this cell mean? It is the percentage similar to a specific location for top-k of real position and top-k of [54, 123]. So, the similarity matrix Sx,y is a matrix of percentages, where every cell represents the percentage similar to that cell and the user position. The user is able to use this result matrix to identify cells where the similarity is within acceptable levels.

To generate the similarity matrix for our proposal, we followed the same method of Dewri to get the matrix, but with some variations. Presumptively we will superimpose a grid containing r rows and c columns on a geographic area $\mathcal{G}$. A new grid will cover 3.2 × 3.2 km2 area with numbers of rows and columns 320 × 320, each cell will be 10 × 10 m area. As a result, the new grid will return the same bandwidth 124.5 that Dewri mentions, but with more precision.

Each cell will correspond to the top-k results and can be represented by one of V symbols. Of course the size of the grid should be substantially larger than V. V is defined as follows:

$$V = \{Rk\ (P,\, Pos\ (x,\, y)) \quad : 1 \le x \le c,\ 1 \le y \le r\}$$

Let Vsim be a matrix that denotes the similarity values for each pair of elements of V:

$$Vsim\ [i,\, j] = Sim\ (Vi,\, Vi),\ Vi\ .\ Vi\ \in V$$

For more explanation, suppose a value V has the next results for top-5

V	V_1	{a, b, c, d, e}
	V_2	{a, b, c, f, g}
	V_3	{f, g, h,i, j}

		V_1	V_2	V_3
V_{sim}	V_1	100	60	0
	V_2	60	100	40
	V_3	0	40	100

To understand how we got Vsim matrix, for example the overlap between V1, V2 is {a, b, c} = 3/5 *100, the result 60% .

As a result, the new matrix is the matrix that the user obtains to determine privacy level. Based on this matrix, a certain level of degree is given, and based on this degree, the inaccuracy levels vary.

B. Transformation the Original Coordinates

Foremost reason the idea of changing the user's location is that, after zooming the similarity matrix, the user's location is exposed, even though with a small size matrix of 3.2 km. Hence, we used LocX equation to modulate the real location to imaginary location. It as follows:

$$(x`,\, y`) =$$
$$(x * cos(\theta\,) - y * sin(\theta\,) + b,\ x * sin(\theta\,) + y * cos(\theta\,) + b)$$

When we apply LocX equation on the single hypothetical value of (x, y) while the fixing b value to be zero. The relationship between (x`, y`) and the angle (θ) is a reverse relationship. When the value of angle (θ) changed, the value of (x`, y`) is declined ever when the rate of angle (θ) increased till 180° value, then the value (x`, y`) start to increase and returned to its original value.

Despite the fact that this equation achieved the needed conditions in providing user confidentiality in LocX application, where it create a new imaginary location, but it will not fit our system. This is because it has no precise results that reach our ambition, and again, this is because the results do not satisfy our system's requirements due to its lack of accuracy in results, whereas that the results we were looking for is near (x, y), and the given result was nowhere near the expected point. As it is well-known mathematically that the value of sin (θ) and cos (θ) range between [-1, 1]. Therefore, when these values are multiplied by (x, y) coefficient, it won't affect the result very much and will only transform it to the negative side of the x-y plane. From this particular point we added some changes to the original equation so that it would fit our new system's criteria. We had to produce a new factor that had an effective outcome on (x', y') values. So an added special range (R) been introduced, and module of the substitution was found out with the result of (x`, y`) out of the original equation. The next step is to get the sum of all of the results from the above mentioned steps with the value of (x, y), respecting the absolute value, so that (x`, y`) doesn't go further away from our original point. Table (1) illustrates the comparison between the LocX equation and our invented equation.

To shorten the new invented equation, a symbols Z was given for (x * cos (θ) – y * sin(θ)), and symbols W for (x * sin(θ) + y* cos(θ)). So, from equation (1):

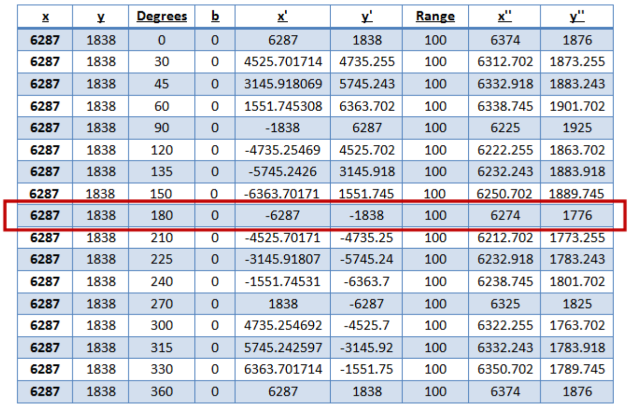
$$(x`, y`) = (Z, W)$$

To generate the new anonymous location, the new equation will be as follows:

$$(x``, y``) = (x + | Z \bmod R| , y + | W \bmod R|)$$

Table (1) shows an example of applying the improvement equation for assumption location with the LocX equation. It is clear that the value of new (x``, y``) lies not far comparatively from the original (x, y). Furthermore, it was found that the greater range being applied, the farther result is found for (x``, y``).

TABLE I. COMPARISON OF RESULTS BETWEEN THE TWO EQUATIONS



x	y	Degrees	b	x'	y'	Range	x''	y''
6287	1838	0	0	6287	1838	100	6374	1876
6287	1838	30	0	4525.701714	4735.255	100	6312.702	1873.255
6287	1838	45	0	3145.918069	5745.243	100	6332.918	1883.243
6287	1838	60	0	1551.745308	6363.702	100	6338.745	1901.702
6287	1838	90	0	-1838	6287	100	6225	1925
6287	1838	120	0	-4735.25469	4525.702	100	6222.255	1863.702
6287	1838	135	0	-5745.2426	3145.918	100	6232.243	1883.918
6287	1838	150	0	-6363.70171	1551.745	100	6250.702	1889.745
6287	1838	180	0	-6287	-1838	100	6274	1776
6287	1838	210	0	-4525.70171	-4735.25	100	6212.702	1773.255
6287	1838	225	0	-3145.91807	-5745.24	100	6232.918	1783.243
6287	1838	240	0	-1551.74531	-6363.7	100	6238.745	1801.702
6287	1838	270	0	1838	-6287	100	6325	1825
6287	1838	300	0	4735.254692	-4525.7	100	6322.255	1763.702
6287	1838	315	0	5745.242597	-3145.92	100	6332.243	1783.918
6287	1838	330	0	6363.701714	-1551.75	100	6350.702	1789.745
6287	1838	360	0	6287	1838	100	6374	1876

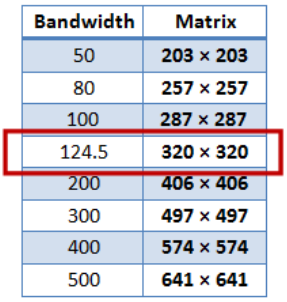
C. *Limitation of Bandwidth*

It is well known that, mobile mapping service application has an effect on the bandwidth. Thus, there is a trade-off between the amount of information transmitted and the bandwidth.

Therefore, there was a tendency to give the user more authorities in addition to the granted privacy authorities given to him. These authorities related to the bandwidth size. The given authorities provide a power to the application through a satisfied selected bandwidth, where the relationship between the bandwidth and the size of matrix is a positive relationship. The user in this case can chose a bigger bandwidth, resulting in a bigger matrix. So, this matrix will cover a larger area, which will provide the user with more choices.

Where Dewri proved that the size of the data sent was generated from the matrix does not affect the quality of the bandwidth and the computation of throughput. Therefore, The size of the matrix 320 × 320 have been adopted as 124.5 which is the size that was mentioned by Dewri. Accordingly, an analysis was done with the goal of determining the relationship between the size of the actual matrix and the size of the individual cells. Then different values started to be generated to calculate different matrices, these values ranging between smaller values than 124.5 and a larger ones. In this way, a freedom of choice was given to the user to select the bandwidth size. Table (2) describe a few examples of bandwidth with the size of matrix that was calculated based on the bandwidth.

TABLE II. THE SIZE OF MATRIX THAT WAS CALCULATED BASED ON THE BANDWIDTH



Bandwidth	Matrix
50	**203 × 203**
80	**257 × 257**
100	**287 × 287**
124.5	**320 × 320**
200	**406 × 406**
300	**497 × 497**
400	**574 × 574**
500	**641 × 641**

V. CONCLUSION

Given the variety of technologies and their key aspects required to operate the LBS available today, a bright future can be forseen. The sheer number of people that this technology can help around the world far outweighs the effort required to create and enhance this technology. Many intruders have vile intentions to threaten and steal user's privacy. Thus it was the ambition of several researchers to find a method and/or technique to shield the user's privacy during LBSs usage.

In this paper, we proposed a supplemental architecture to successfully address some of the inherent limitations of previous works. Improving the granularity of the previous similarity matrix was one of the great upgrades that improved the system. That was done by focusing the new similarity matrix in an area close to the original point. The system achieved better performance by not threatening the accuracy of the system without the requirements of providing results at such as sparse level. The improvements now give the user true and complete flexible control over their privacy and the system.

REFERENCES

[1] R. Dewri and R. Thurimella, "Exploiting Service Similarity for Privacy in Location-Based Search Queries," IEEE Transactions On Parallel And Distributed Systems, vol. 25, no. 2, pp. 374 - 383, FEBRUARY 2014.

[2] J. Schiller and A. Voisard, Location-Based Services, Amsterdam: Elsevier, 2004.

[3] A. Malm, "http://gwtechinc.com/business-models-shift/," 2014. [Online].

[4] F. Grace, "Stalker Victims Should Check for GPS," CBS Broadcast Center, February 2003. [Online]. Available: http://www.cbsnews. com.

[5] K. G. SHIN, X. JU, Z. CHEN and X. HU, "Privacy Protection For Users Of Location-Based Services," IEEE Wireless Communications, vol. 19, no. 1, pp. 30 - 39, February 2012.

[6] R. Dewri, "Beyond the Thin Client Model for Location Privacy," in International Conference on Privacy and Security in Mobile Systems, Atlantic City, June 24-27, 2013.

[7] R. Dewri, "Can a Phone's GPS Lie Intelligently?," IEEE Computer Magazine, vol. 46, no. 2, pp. 91-93, 2013.

[8] R. Dewri, "Local Differential Perturbations: Location Privacy Under Approximate Knowledge Attackers," IEEE Transactions on Mobile Computing, vol. 12, no. 12, pp. 2360-2372, 2013.

[9] R. Dewri, "Location Privacy and Attacker Knowledge: Who Are We Fighting Against?," in 7th International ICST Conference on Security and Privacy in Communication Networks, London, UK, September 7-9, 2011.

[10] R. Dewri, "Query m-Invariance: Preventing Query Disclosures in Continuous Location-Based Services," in 11th International Conference on Mobile Data Management, Kansas City, Missouri, USA, May 23-26, 2010.

[11] T. Tsiligiridis, C. Pontikakos and T. Glezakos, "Location-based services: architecture overview," in ITAFE, Turkey, 2005.

[12] D. Mohapatra and S. S.B, "Survey of location based wireless services," in IEEE International Conference on Personal Wireless Communications, 23-25 Jan. 2005.

[13] E.-S. Lohan, O. Cramariuc, A. Rusu-Casandra and I. Marghescu, "User requirements in the context of future location based services as seen from a survey among Romanian students," in International Conference on Localization and GNSS (ICL-GNSS), Tampere, Swedish, 2011.

[14] R. Rizia, M. Tanviruzzaman and S. Iqbal Ahamed, "KnockAround: Location Based Service via Social Knowledge," in 36th International Conference on Computer Software and Applications, Izmir, 2012.

[15] J. Zhang and E. Mao, "Management of Location-Based Services Innovation: Insights from Consumers," in Innovation Conference (SIIC), Beijing, 2013.

[16] M. Wernke, P. Skvortsov, F. Durr and K. Rothermel, "A classification of location privacy attacks and approaches," Parallel and Distributed Systems, IEEE Transactions, vol. 20, no. 4, pp. 512 - 527 , 2009 .

[17] A. Khoshgozaran, H. Shirani-Mehr and C. Shahabi, "SPIRAL: A Scalable Private Information Retrieval Approach to Location Privacy," in Mobile Data Management Workshops, Beijing, 2008.

[18] M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," in Third Int'l Conf. Pervasive Computing,, Berlin, 2005.

[19] G. Ayres and R. Mehmood, "LocPriS: A Security and Privacy Preserving Location Based Services Development Framework," in Knowledge-Based and Intelligent Information and Engineering Systems 14th International Conference, Cardiff, UK, September 8-10, 2010.

[20] H. Kido, Y. Yanagisawa and T. Satoh, "An anonymous communication technique using dummies for location-based services," in International Conference on Pervasive Services, 2005.

[21] A. Suzuki, M. Iwata, Y. Arase, T. Hara, X. Xie and S. Nishio, "A user location anonymization method for location based services in a real environment," in 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2010.

[22] R. Kato, M. Iwata, T. Mayu, A. Suzuki and Y. Arase, "Dummy-based Anonymization Method Based on User Trajectory with Pauses," in ACM SIGSPATIAL GIS'12, 2012.

[23] A. Pingley, N. Zhang, X. Fu, H.-A. Choi, S. Subramaniam and W. Zhao, "Protection of Query Privacy for Continuous Location Based Services," in INFOCOM, Proceedings IEEE, Shanghai, 2011.

[24] N. Yang, Y. Cao, Q. Liu and J. Zheng, "A Novel Personalized TTP-free Location Privacy Preserving Method," International Journal of Security and Its Applications, vol. 8, no. 2, pp. 387-398, 2014.

[25] M. Mokbel, C.-Y. Chow and W. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," in VLDB Endowment, Seoul, Korea, 2006.

[26] B. Bamba, L. Liu, P. Pesti and T. Wang, "Supporting Anonymous Location Queries in Mobile Environment with Privacy Grid," in the International World Wide Web Conference committee, Beijing, China, April 21-25, 2008 .

[27] M. Mano and Y. Ishikawa, "Anonymizing user location and profile information for privacy-aware mobile services," in 2nd ACM SIGSPATIAL International Workshop on Location Based Social Networks, 2010.

[28] K. Miura and F. Sato, "Evaluation of a Hybrid Method of User Location Anonymization," in Broadband and Wireless Computing, Communication and Applications (BWCCA), Compiegne, 2013.

[29] B. Bamba, L. Liu, P. Pesti and T. Wang, Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid, Beijing, China: e International World Wide Web Conference committee (IW3C2), April 21-25, 2008.

[30] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Distributed Computing Systems, Columbus, OH, 2005.

[31] G. Zhong, I. Goldberg and U. Hengartner, "Louis Lester and Pierre: Three Protocols for Location Privacy," the Natural Sciences and Engineering Research, Canada, 2007.

[32] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg and D. Boneh, "Location Privacy via Private Proximity Testing," in Network Distributed System Security, 2011.

[33] X.-Y. Li and T. Jung, "Search Me If You Can: Privacy-preserving Location Query Service," in INFOCOM, Proceedings IEEE, Turin, 2013.

[34] W. Wong, D. Cheung, B. Kao and N. Mamoulis, "Secure kNN Computation on Encrypted Databases," in the 35th SIGMOD International Conference on Management of Data, Rhode Island, USA, June 29–July 2, 2009.

[35] R. Dingledine, N. Mathewson and P. Syverson, "Tor: The Second-Generation Onion Router," in Proc. 13th Con, Berkeley, CA, USA, SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium .

[36] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Order Preserving Encryption for Numeric Data," in International Conference on Management of Data, 2004.

[37] K. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel and B. Zhao, "Preserving Location Privacy in Geosocial Applications," Mobile Computing, IEEE Transactions, vol. 13, no. 1, pp. 159 - 173, 2014.