International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 5, September – October (2015)

RESEARCH ARTICLE

A Fine-Grained Spatial Cloaking With Query Probability Levels for Privacy in LBS

Albelaihy Abdullah
Department of Computer Science, King Abdul-Aziz University.
Abu_meteb30{at}hotmail.com

Jonathan Cazalas
Department of Computer Science, College of Computing and Information Technology, King Abdul-Aziz University.
jcazalas{at}kau.edu.sa

Abstract – In the technology of LBS i.e. location based services, location related queries are submitted to the mobile users. These queries are submitted to untrusted server of LBS for obtaining service. However, these queries considerably stimulate and produce privacy issues associated with mobile users. FGcloak has been proposed so as to address this privacy related issue. It has been revealed that the FGcloak is considered as the fine grained spatial cloaking method based on the query probability levels to generate k-anonymity used for the privacy aware mobile users in the location based services. The modified Hilbert Curve is used so as to efficiently guarantee k-anonymity and simultaneously offers bigger cloaking region.

Index Terms---LBS, FGcloak, fine grained spatial cloaking, location based services.

1. INTRODUCTION

LBS i.e. location based services have found to be well accepted in recent era. It is due to the advent of modern mobile devices like tablet as well as smartphones [1] [2]. The increased use of these modern devices has increased the usage of location based services in current technological age [1]. Mobile users have become common which has resulted in increased opportunities for communication as well as improved awareness related to the surroundings [3]. It has been found that with the help of Google play store or Apple store, users are capable of downloading and installing location based applications in their smart devices such as tablets and smartphones, It allows the mobile users to submit their queries to the server of LBS [4] [5]. As a result of which; mobile users become capable of obtaining location related service data regarding POIs i.e. Point of Interests within the vicinity. For instance, mobile users become capable of efficiently looking for the nearby banks or clinics and they easily verify the information related to the price of the nearby Red Lobster restaurant. With the expansion of mobile devices like tablets and smart phones, location based services (LBSs) are being used increasingly. Basic use of location based services is to offer simple ways for location aware information retrieval and location information sharing. Hence, LBSs are considered to be convenient and useful.

However, these services pose stern risk to the privacy of users as these services tempt to disclose their locations to the service providers. The information of the location of users is disclosed through the queries which are provided for gathering location based information. There is a great significance of protecting the privacy of users from LBS providers in order to ensure the effectiveness and wellbeing of LBS ecosystem. In this way, the market of LBS will prosper and expand as users may find themselves comfortable while the use of LBS. Besides several benefits, LBS pose serious risks to the privacy of users. Through gathering information of user's location entrenched in the queried of LBS, the opponent can deduce sensitive privacy information related to the recipients of service. The two types of privacy issues related to LBS include location privacy and query privacy. For instance, the user lives in some rural area. The user may disclose his/her location information in terms of large area in response to the query. This will allow preserving the location privacy of user.

Generally, the servers of location based services serve a user-based in response to their submitted query of location based services [1] [6] [7]. For instance, if the user queries "show me the information of restaurant within one mile", then the server responds to this query of the mobile user. This query includes query an interest pair and the location. It can also contain some other meaningful information such as the ID of user, query radius etc. Though, it is revealed that such kind of submitted information can be abused by the unreliable severs of location based services (including other parties who compromise with the servers) [2] [8] [9] [10]. Thus, it has been observed that with the help of location based services, the location of the mobile user can be identified by the server. In addition to this, the types of queries being submitted to the servers can also be found by untrusted servers of location based services. Moreover, these servers can further determine that what the mobile user is doing etc. [11] [12] [13] [14]. Hence, it can be said that the use or integration of location based services can track the mobile users as well as release the personal information of the

RESEARCH ARTICLE

mobile users to 3rd parties like advertisers [15]. Hence, ensuring the protection of the privacy of the mobile users appears to be highly significant and essential. Usually, the LBS servers serve a user, and depends on its presented LBS query (e.g., show us the clinic information inside 1 mile), which usually contains (location, query interest) binary and maybe some other information like the user's ID and query radius, etc. Nevertheless, these presented information could be misused through the untrusted LBS servers. Thus, the LBS servers could know where the users is, and which type of queries they present, and what they are doing, etc. They can follow users or cast their special information to third parties like advertisers. So, we need to pay more concern to protecting privacy.

In order to resolve as well as overcome the issues related to the protection of privacy of the mobile users, a number of techniques have been proposed in recent age within the literature. According to the research of [16], it has been revealed that the modern and recent techniques for dealing with privacy issues can be categorized into two main types. These types include mobile devices based schemes and trusted anonymization server based schemes [4] [5]. According to the study of [14], it has been observed that the most common and widespread approach being used, for resolving the privacy concerns, is attaining *k-anonymity*. It has been investigated by the research that the approach of k-anonymity makes use of obfuscation and location perturbation. In addition to this, this approach also makes use of dummies or spatial as well as temporal cloaking. According to the studies of, it has been found that spatial and temporal cloaking is the most common and useful scheme amongst all of the other schemes. This scheme is being used in effective and efficient manner in real smartphones so as to ensure the privacy of the mobile users using smartphones [13] [14]. According to the studies of [4] [17], it has been observed that these schemes assist in minimizing the cloaking region so as to minimize the system overhead.

This scheme further assists in maximizing the cloaking region for the ensuring the provision of improved privacy of the information of mobile users [13] [16] [17] [18]. According to the studies of [5] [19] [20], it has been found that trusted anonymization server based schemes are being used extensively and widely in order to protect the privacy of the mobile users of smartphones. So with this scheme, the query is coming from the mobile user is presented to the server of location based services with supporting by the trusted 3rd party server (again with this example, location anonymizer). Thus, this technique helps in expanding the queried location into the bigger cloaking region as it covers k – 1 other mobile users for achieving the k-anonymity [1] [14]. Through this scheme, the unreliable servers of location based services are not capable of identifying the real location of the users. Thus, the inclusion and integration of this scheme assists in the provision of trusted server. It becomes the system's weak point and appears as the single point of the failure. According to the studies of [19] [21] [22] [23], it has been revealed that the mobile devices based schemes assist in removing the trusted server through the construction of the cloaking region on the basis of the information of exchanged location from other encountered users. Certain limitations have been found related to both of the schemes. However, both are being used in effective and efficient manner through the enhancing overall performance of these schemes. It has been found that this scheme includes existing solutions which offer users with the maximum or the minimum possible cloaking region [7], [10]. However, the insufficient and inadequate balanced consideration amid constrained resources of mobile devices as well as required privacy level of the mobile users. But, this scheme confronts with the challenge of finding enough and adequate users within the practical cloaking region. Different solutions have been proposed in order to deal with the privacy issues of LBS. several techniques which can be used for the protection of user's data. K-anonymity is the most famous metric which is being deployed in order to ensure the privacy protection of LBS query [16]. This technique signifies that k-anonymity protection of a release is provided if the information enclosed in each release for each person can't be differentiated from at least K-1 individuals, whose information seems to be present within the release. Different approaches have been adopted for using this metric.

These approaches include spatio-temporal cloaking boxes and spatial cloaking boxes. In addition, location entropy is also considered as the most useful technique for protecting user's privacy of LBS. The article further suggested policy based schemes for ensuring the protection of data privacy of users. Location obfuscation and perturbation schemes have also been suggested [16].

According to the study of [20] [24] [25], it has been revealed that the PIR i.e. Private Information Retrieval approaches are also used for providing more powerful and more generalized method of blinding the un-trusted location server through the conversion of spatial query processing into a number of private database retrievals with the help of location servers. It has been found that the use of PIR protocol assists in allowing the client for secretly requesting the record which has been stored within an un-trusted server without exposing the retrieved record to un-trusted server. Thus, rather blurring the queries of users, PIR is used for the protection of the queried content. Hence, in this way, there remains no information which leaks to adversaries through scrutinizing the requested records from un-trusted server. The use of cloaking approach can assist in protection the location of the user through hiding the information of the user. In this way, cloaking approach assist in enabling location based services through the provision of security solutions without the need

RESEARCH ARTICLE

of trusted third party. This paper emphasized on the design of such protocol which must be used for controlling the access of entities. The control related to the access of the user's information not allow any unauthorized party to reveal the location information of any user.

According to the studies of [20] [22], it has been revealed that this scheme assists in protecting the privacy of the mobile users with the help of the integration of larger cloaking regions as well as k-anonymity. It has been further observed through the studies that this scheme can also allow the reduction in the system overhead. It is due to the Hilbert Curve's dimension reduction characteristic [15] [26]. The studies have further found that with the help of FGLR i.e. Fine-Grained Local Replacement algorithm, mobile users are offered with fine grained control over the system's overhead. It is due to the fact that FGLR combines encounter based as well as dummy based approaches.

Thus, in order to avoid all of these issues and to overcome the privacy issues of the mobile users using location based services, the fine grained spatial cloaking scheme has been proposed [23]. This scheme is also termed as FGcloak. In this scheme, the k-anonymity is achieved for the mobile users using location based services. As a result of which, this scheme assists in the provision of the fine grained control over the system's overhead. According to the studies of [11] [27], it has been found that unlike other approaches, the scheme of FGcloak [27] makes use of algorithms so as to carry out fine grained spatial cloaking. The studies have revealed the fact that this scheme makes use of MHCA i.e. Modified Hilbert Curve Constructing algorithm. This algorithm is used because of the fact that it allows in completely filling the considered area of map on the basis of the query probability of the mobile users. This scheme further assists in the provision of k-anonymity as well as guarantees larger cloaking region. This cloaking region makes use of the PADS i.e. Privacy Aware Dummy Selection algorithm so as to warily and cautiously separate the modified Hilbert curve into K number of segments. Lastly, this scheme makes use of the FGLR i.e. Fine Grained Local replacement algorithm for reducing the systems overhead. This system overhead is minimized or reduced with the help of the personalized requirements of the mobile users. Build a modified Hilbert Curve depending users' query distribution, and design a spatial cloaking scheme depends on it to protect user's location privacy in LBSs. This method protects privacy over k-anonymity and big cloaking regions. So, depends on dimension lowering property of Hilbert Curve, then the system overhead can also be minimized. Hence, this scheme gives a good contribution, by the Fine-Grained Local Replacement (FGLR) algorithm which combines dummy-based with encounter-based approaches, it is present users with fine-grained controls on system overhead. It is present over security analysis and wide evaluation results to see the effectiveness, and the efficiency of FGcloak.

Our idea to cover all the maps over three of levels one of them is used with higher query probability and higher density (previous example) but with condition, if the query probability (qp) high, so will divide the cell to 4 point of finer grains (E.g. quadrant technique)= k, Or, if the query probability medium will divide the cell to 4 finer grains also with same technique = k, and if the query probability low will divide the cell to 2 finer grains =k.

Our Modified Hilbert Curve will use for the development of FGcloak [26] on the basis of query probability levels for ensuring the protection of the user's privacy in each of cell, and is not necessary with high query only, thither important and private information in these cells with medium and low query probability needs to protect it and to obstacle for the adversary to discovered.

In general, our contributions are as follows:

- Most of users' queries distributions in local map is covered.
- Privacy increases in the medium and the lower query probability which contains of important data and private information, so that's an obstacle for the adversary to discovered.
- FGloak scheme become more effective.

The remainder of the paper is organized as follows, related work, preliminaries, motivation and basic idea, our fine-grained cloaking scheme, proof of our improvement, conclusion.

2. RELATED WORK

For the protection of the location privacy of the mobile users within location based services, a number of research solutions have been suggested in recent years, according to [2] [3] [16]. From these studies, it has been revealed that the majority of the research solutions offer anonymity on the real locations of the mobile users, for example, k-anonymity, as stated by the study of [14]. The integration of k-anonymity allows hiding the real information of the mobile user into k – 1 other mobile users. According to the studies of [9] [28], it has been found that entropy bases metrics are also being used widely in order to ensure the protection of the privacy of mobile users. On the whole, the privacy of the user's location can be preserved or protected with the help of location obfuscation and perturbation [3][7]. It can further be protected with the help of dummies or spatial as well as temporal cloaking. According to the study of [5], it has been observed that the k-anonymity has been introduced in order to protect the privacy of the user's location. This technique

RESEARCH ARTICLE

hides the real location of the mobile user so as to ensure the provision of location privacy to the mobile users [8] [22].

There are two kinds of algorithms which are used for cloaking. These include Grid based and R-tree based algorithms. The study of [20] has proposed the algorithm of R-tree, which is also termed as CliqueCloak. This algorithm presumes different requirement of k-anonymity for every user [22]. In this algorithm, the collection of users is combined and the CliqueCloak is developed for deciding that whether users are capable of sharing a cloak spatial region or not [24]. However, this algorithm requires a lot of time for constructing the clique graph, which appears as its major limitation [25] [26]. As a result of which, overall response time to the user is boosted through this algorithm. CliqueCloak is the technique which helps in constructing the graph for all of the requests which have not been yet anonymized. In this technique, when any new request is received by the server, it endeavors for identifying the clique including certain existing requests as well as new request. Afterwards, they cloak these requests together within the similar region. There are several disadvantages of using this technique. Limitation of the effectiveness of this technique is the major drawback of this technique. Thus, this technique makes it difficult for finding the anonymity set for such requests which hold large K values [29]. In addition to this, the cost required for the search of clique within the graph is also high, which is another major drawback of CliqueCloak. Furthermore, there are still some requests which are not capable of being anonymized. These requests are dropped when their existence expires. Therefore, there is a great significance of making effective and careful use of CliqueCloak technique in order to attain major goals of this technique.

The study of [18] reveals that the model of Clique Cloak is considered as the personalized k-anonymity model which assists in allowing the mobile users to regulate their anonymity levels. Though, it has been found that this technique makes use of location anonymizer for the generation of the cloaking region. It depicts the anonymizer as the performance bottleneck as well as crucial point of failure.

The study has been found the fact that cloaking algorithm assists in constructing spatio-temporal cloaking boxes which are comprised of at least k number of users. Afterwards, these boxes are submitted to the server of location based services as the locations of the mobile users [8] [15] [22] [26].

According to the study of [20], it has been observed that dummy locations have been proposed for achieving anonymity for avoiding the anonymizer. These dummy locations further emphasize on the reduction of the communication overhead. In addition to this, this technique makes use of random walk model for the generation of dummy locations, which do not ensure the provision of the protection of privacy [18]. It ensures the protection of the privacy of mobile user when the side information of the user appears to be available to the opponent, as states by [1] [22] [30]. Moreover, the study of [20] has proposed the privacy preserving cloaking scheme. This scheme can help in the attainment of k-anonymity through the provision of larger cloaking region. It has been further observed by the study that this scheme needs the phase of warm-up. As a result of which, it will not provide protection of the user's privacy all the time [8] [31]. Thus, these problems take place in the use of trusted anonymization technique. Identical issues also occur in encounter based solutions like EPS and SMILE, as stated by the studies of [8] [31]. In addition to these schemes, the policy based solutions as well as cryptography based schemes have also been suggested for the protection of the privacy of the user's personal information [15] [26].

The study of [27] has revealed that grid depended cloaking algorithms can be categorized into two major categories including Hilbert Curves and Quad-tree curve. The study of [20] has suggested, the promising quad-tree based on the cloaking algorithm. It has been revealed by the study that a space is made up of partition into quadrants unless the number of points in every quadrant attains the K value in quad tree based algorithm. Great time complexity is imposed by this algorithm which is considered as the major drawback or limitation. The time complexity takes place when the observations traverse all through the tree.

The study of [24] has proposed another quad tree based cloaking algorithm which is termed as NewsCasper. An anonymizer helps in maintaining a hash table on the basis of user ids within this algorithm [24] [25] [32], user ids within this algorithm. These user's ids point to the lowest level quadrant in which the user lies. Thus, the location of each and every user can be accessed in direct manner through preventing top down access of Quad tree. Generated cloaking region appears to be large which is considered as the major problem of Quad tree algorithm. It is due to the fact that quad tree algorithm splits the space into several quadrants. Dealing with more POIs candidates is needed, which degrades query processing performance [20] [22] [33]. For overcoming the issues related to Quad tree based algorithms. In addition to this, the study of [24] has further proposed the Hilbert-Curve based cloaking algorithm. PRIVE and MOBIHIDE are the two major frameworks which have been proposed by this cloaking algorithm. In the proceeding research, Hilbert Curve will be used [4] [34]. The major benefit related to the use of Hilbert Curve is that it assists in guaranteeing the user's anonymity as well as assists in generating small cloaking region as compared to Quad tree. However, on the other hand, the major limitation related to Hilbert Curve is that the cloaking region can be raised needlessly because of the

RESEARCH ARTICLE

extension related to adjacent cells through the use of sequential identifiers of Hilbert Curve [15] [22] [25].

There are two major techniques which are used for mapping the cloaking region. These techniques include quad tree mapping and other is Various-Size- Grid Hilbert Curve (VHC) mapping [20] [22] [26]. In specific, this technique assists in resolving the problem related to the POIs density which varied with respect to geographic area.

It has been further investigated by the study of [35] that there are several different schemes which make use of Hilbert Curve, for instance, Mobihide. However, majority of the schemes use standard Hilbert Curve which differs from the modified Hilbert Curve. The modified Hilbert Curve which has been used in this study is identical to VHC i.e. Various-grid-length Hilbert Curve deployed in CAP [1] [2] [10] [21]. However, there are some differences as well which have also been highlighted in the study. The major difference is that the VHC is developed with the help of road density; whereas, the modified Hilbert Curve is developed with the help of query distribution [26]. In addition to this, VHC is deployed for perturbing the single location; however, the modified Hilbert Curve is deployed for the selection of dummy locations. Furthermore, the use of modified Hilbert Curve assists in the provision of fine grained control over the system overhead but CAP does not include this characteristic.

So with [27], a fine gained cloaking for the privacy aware user, the modification within the Hilbert Curve has been introduced which assists in the provision of effective and efficient k-anonymity protection. In order to carry out this technique, the standard Hilbert Curve will be modified in accordance with the query distribution based on high query probability only. Standard Hilbert Curve spanning whole local map As the distribution of all queries submitted by mobile users within the local map might not be uniform; thus, there is a great significance of modifying standard Hilbert Curve which considers the query probability, it has been found that trusted anonymization server based schemes are being used extensively and widely in order to protect the privacy of the mobile users of smartphones. As for Fine-Grained Local Replacement Algorithm, to adjust the cost of information exchange, so we can use a parameter exchange ratio (indicated by σ), [27]:

$$ratio,\ \sigma = \frac{t_{no.2} - t_{no.1}}{t_{no.2} - t_0}, 0 < \sigma < 1. \quad (1)$$

This parameter measures the fraction of time by which a user exchanges information with other encountered users which depends on the available resources. In general, bigger indicates that's mean more chances of communicating with encountered users, and with higher communication cost too. By this technique, the untrusted servers of location based services definitely not be able of identifying the real location of the users.

It has been revealed that high probability of query results in finer grains, it has been planned to carry out modification of standard Hilbert Curve in accordance with finer grains within the region, along with high distribution of query. The Figure 1 is representing the modified Hilbert Curve [27].

3. PRELIMINARIES

This section of the paper will emphasize on the adversary model as well as basic concept which will be incorporated into the paper. The basic idea related to the scheme will also be highlighted in this section.

3.1. Basic Concept

Query probability information within the local map of the user is the information which will be used for accomplishing this paper. Particularly, presume that the local map is categorized into cell's seat (i.e. n*n cells). According to the studies of [19] [27], it has been found that the query probability within the specific cell can be signified like the probability with which users submit location based queries from the specific cell.

3.2. Adversary Model

There is major type of adversary which have been considered in this research paper. This type is active adversary.

- Active Adversary

Such entity can become active adversary when it can compromise the server of location based services as well as acquire all the information which is preserved into the server for performing attacks like inference attack. In this research paper, the server of location based services is assumed to be active adversary. Thus, the entity can retrieve the information of each user as well as track the queries submitted by the mobile users. With the help of this technique, the user's historic data and situation can be obtained. This technique makes use of location privacy protection algorithm so as to ensure the protection of the personal information of mobile users [27].

3.3. Motivation and Basic Idea

According to the studies of [11] [27], it has been revealed that mobile users within the present applications of location based services are required to submit queries to the server of location based services for obtaining service data. The usual query incorporates exact location, identifier, query range as well as query interest of the user etc. But, this data of the mobile users might release sensitive information of the user to either public or adversaries [1]. It has been found that for the protection of the privacy of mobile users, the technique of k-anonymity is being used widely, but this technique

RESEARCH ARTICLE

encompasses a number of drawbacks. Thus, these drawbacks need to be prevented which are associated with the k-anonymity based solutions [22] [34]. The major problem which has been found is caused by the 3rd party server used in existing techniques (such as location anonymizer) [4] [19]. This problem appears as the bottleneck to the performance of system as it presents privacy concerns. Another effective solution which has been proposed is the provision of fine grained control for the mobile users for tuning the trade-off amid privacy and system overhead on the basis of the limited resources of the smartphones. In addition to this, the study of [22] has revealed the fact that the cloaking region's size cannot always be assured. It has been further stated in the study that the cloaking region's size cannot be assured especially when the system is in the phase of warming up or when the encountered number of users are less.

For attaining the fine gained cloaking for the privacy aware user, the modification within the Hilbert Curve has been introduced which assists in the provision of effective and efficient k-anonymity protection [26]. In order to carry out this technique, the standard Hilbert Curve will be modified in accordance with the query distribution and based on the high query probability [7]. Standard Hilbert Curve spanning whole local map has been depicted in the Figure1. As the distribution of all queries submitted by mobile users within the local map might not be uniform; thus, there is a great significance of modifying standard Hilbert Curve which considers the query probability.

According to the studies of [27], it has been revealed that high probability of query results in finer grains. Thus, it has been planned to carry out modification of standard Hilbert Curve in accordance with finer grains within the region, along with high distribution of query. The Figure1 is representing the modified Hilbert Curve.

According to the studies of [12] [17] [22], it has been observed that the Hilbert Curve encompasses a unique property. This property is that the two closest points within the planned space are probable to be close to the original space [12]. This characteristic of the Hilbert Curve assist in the development of cloaking region within the location based services. As the development of larger cloaking region is preferred; thus, it is essential to avoid adjacent points within the Hilbert Curve. For attaining this goal, k segments of modified Hilbert Value have been made. For instance, the real location of the mobile user is one segment. Afterwards, from k-1 segments, almost k-1 candidates have been chosen. In this manner, the selected candidates are capable of covering the biggest possible are within the local map, under the limit of K. in this way, there are k-1 candidates available for attaining k-anonymity, while assuring the required cloaking region. In addition to this, the dummy locations for each selected candidate can also be generated. However, it appears to be difficult for guaranteeing the efficiency for k-anonymity. It is due to the fact that there are certain locations which are dubious to be real (for example: swamps, rugged mountains and lakes). More practical anonymous set can be collected through the history locations of the mobile users. But, this technique may cost high on the basis of computation, storage and communication.

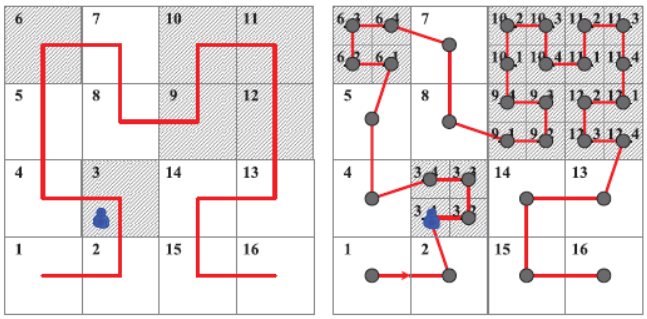
3.4. Resistance to Inference Attack

Theorem. With our scheme is inference attack resistant.

Proof: As for active adversary, with a few basic knowledge, it defines the proposed scheme and the related algorithms. First of all, recall our PADS algorithm. Every candidate is chosen from the cell with same rank in each segment. So, in this technique could confuse the powerful active adversary. For the active adversary's knowledge, it can execute our scheme for k tests. The best result is that he cannot distinguish the real user from others based on the testing results. In our scheme, for a presented cloaking region which covers k locations, the active adversary can choose any one as the observed real user and perform our scheme. Clearly, it can obtain the same set of locations for constructing cloaking region. Wherefore, it is difficult for the adversary to reverse our algorithm [27].

4. OUR FINE-GRAINED CLOAKING SCHEME

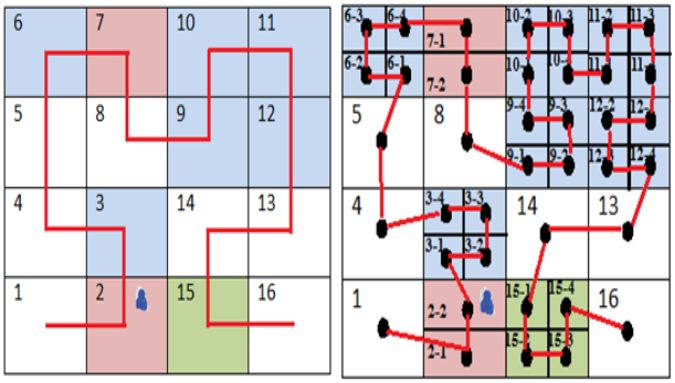
In this section, we present our proposed FGcloak based on query probability levels, then, we introduce the details. Next in [27] and based on this modified will make our extended. We provided the Figures 1,2 and 3 with our solution, in Figure1 we can realized the local map with high query, while within Figure2 we can realizes that local map is covered by three of colours: one with blue is represented high query probability, and the second with green is represented medium query probability, and the third is pink represented low query probability. Depends on the standard Hilbert Value (as you can see in Figure. 2(a) and (b)) of the standard Hilbert Curve. In Figure1. This scheme is also termed as FGcloak [27].



(a) Standard Hilbert Curve (b) Modified Hilbert

Figure. 1. Modified Hilbert Curve [27]

RESEARCH ARTICLE



(a) Standard Hilbert Curve (b) Modified Hilbert Curve

Figure. 2. Our Modified Hilbert Curve based on query probability

4.1. Modified Hilbert Curve Constructing Algorithm

In general, the query probability in our local map it's possible to get from other third parties, For example one of the social network applications. All of these information the mobile user could construct a modified Hilbert Curve then modify our extended on it, which indisputably covers most of map with different grains. So let us take previous example shown in Figure. 1. Especially in Figure. 1(a) we can see the standard Hilbert Curve where the queries are uniformly distributed in the map. With Figure. 1(b), Assume the query probability INSIDE 1st region is a (benchmark), denoted as 1. And the 2nd region's query probability is likeness to the 1st region, also denoted 1 too. The query probability INSIDE the 3rd region is much higher, so, 4 times of the benchmark. Thus, we split the 3rd region into finer grains (e.g., by quadrant technique), then mark them as 3-1, 3-2, 3-3 and 3-4 sequentially.

Herewith above example, we can see the modified Hilbert Curve really constructed. So, we can realize the Hilbert Curve covers the regions but only with higher query probability and higher density.

Based on that, our idea to cover all the maps over three of levels one of them is used with higher query probability and higher density (previous example) but with condition, if the query probability (qp) high, so will divide the cell to 4 point of finer grains (E.g. quadrant technique)= k, Or, if the query probability medium will divide the cell to 4 finer grains also with same technique = k, and if the query probability low will divide the cell to 2 finer grains =k. With Figure. 2(b), Assume the query probability INSIDE 1st region is a (benchmark), denoted as 1. And the 2nd region's query probability is low, so we split the region into finer grains and mark them as 2-1, 2-2, just like that in 7th. Then the query probability INSIDE the 3rd region is higher, so, we make it 4 times of the benchmark.

Hence, we split the 3rd region into finer grains (example: used with quadrant technique), then mark them as 3-1, 3-2, 3-3 and 3-4 sequentially. Just like that in, 6th, 9th, 10th, 11th, 12th regions, partitioned to finer grains too. While in 15th the query probability INSIDE cell is medium, so will split the 15th region into finer grains (example: used with quadrant technique) too. Thus, mark them as 15-1,15-2,15-3,15-4.

4.2. Privacy-Aware Dummy Selecting Algorithm

Depends on the standard Hilbert Value (as you can see in Figure. 2(a)) of the standard Hilbert Curve, so we can easily calculate the modified Hilbert Value (as in Figure. 2(b)) through region quadrants. But we initially count the total number ($N_{average}$) of the cells regardless of their sizes, after that equally divide them into k segments (as in step 2 within Figure. 3(b)). And the average number $N_{average}$ of cells in every segment can be calculated by [27]:

$$N_{average} = \left[\frac{N_{total}}{k} \right]. \quad (2)$$

Whereby to the rank (say r) for real user (c_{real}) inside its segment (for example. r = 1 if it is the first component of the segment), so we can pick the r^{th} component of every the remaining k − 1 segments. So, we can use the chosen components as the k−1 candidates. For instance, suppose we try to achieve 6-anonymity, in Step 1 of the example in Figure. 3, so the total number of the cells will be $N_{total} = 39.$ Then we can compute: $N_{average} = \left[\frac{N_{total}}{k} \right] = \left[\frac{39}{6} \right] = [6.5] = 7.$

In Step 2, of the example in Figure. 3, we can divide the modified

RESEARCH ARTICLE

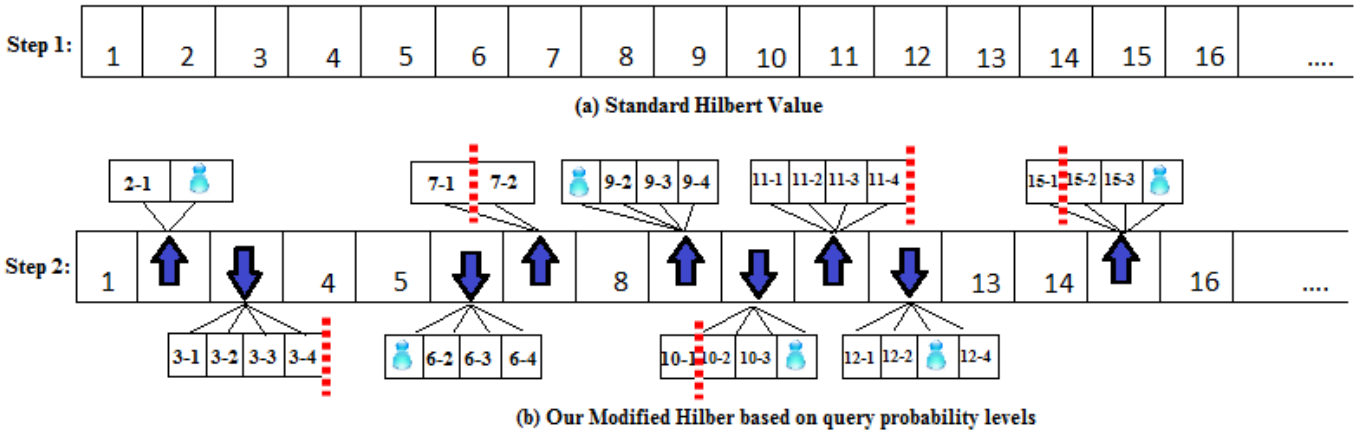


Fig. 3. Our Solution

Hilbert Value into 6 segments as 1 ~ 3-4, 4 ~ 7-1, 7-2 ~ 10-1 , 10-2 ~ 11-4, 12-1~ 15-1 and 15-2 ~ 16. After that, then depends on the rank of the real user c_{real} in its segment which is 3, so we choose the third cell (2-2, 6-1, 9-1, 10-4,12-3 and 15-4, respectively) in every segment as the other 5 candidates.

5. PROOF OF OUR IMPROVEMENT

Now, we need to proof our scheme within each of cell, we need to calculate the query probability. *P=(p1,..,p3,pm), and Q=(q1,..,q3,qm)*, if the query probability is high then divided to fine grained then count the k-Anonymous and the "entropy", and the same with cells which has medium query probability and lower of query probability. Then get the sum of k-Anonymous for three of levels.

Lemma 1.1. Let query probability (qp) high, and the Q is the specific number of query, if the qp $\geq$ Q then calculate that inside the cell.

Lemma 1.2. Let query probability (qp) medium, and the Q is the specific number of query, if the Q > qp $\geq Q_1$ then calculate that inside the cell.

Lemma 1.3. Let query probability (qp) lower, and the Q is the specific number of query, if the qp $< Q_1$ then calculate that inside the cell.

Lemma 1.4. Let *pji* the query probability inside the cell and denoted as *pj1, pj2, pj3, ..., pji, .., pjk* and we can calculated by[22]:

$$pji = \frac{qji}{\sum_{l=1}^{k} qjl}, i = 1,2...,k, \qquad (1)$$

Lemma 1.5. Let qi, the total of queries in the local map and computed by [22]:

$$qi = \frac{\#of\ queries\ inside\ cell\ i}{\#of\ queries\ in\ all\ map}, i = 1,2,...,n^2 \quad ---(2)$$

Where $$\sum_{i=1}^{n^2} qi = 1$$

Proof. Let (h) high, (m) medium, (l) low, and (qp) the query probability:

$$qp = \frac{\#of\ queries\ inside\ cell\ h+m+i}{\#of\ queries\ in\ all\ map} i = 1,2,...,n^2 \quad --(3)$$

Lemma 1.6. Let *H* entropy, and considered as measure the level of k- anonymity and Entropy is a measure of the average degree of uncertainty associated with a set of events. Formally, the entropy of a set of N events, so we can achieve the max of entropy $H_{MAX} = \log_2 k.$ [22] by:

$$Hj = -\sum_{i=1}^{K} Pji.\log_2 pji. \qquad (4)$$

Where *Pji* is probability of occurrence event i.

Theorem 1. Let KAA is the (k-Anonymity Accuracy), to measure the k-Anonymity for each cell by the equation in [36] denoted as KNN:

$$KKA = \frac{The\ no.of\ Moving\ object\ in\ Cells}{k\ user\ of\ no.\ of\ request} ---(5)$$

RESEARCH ARTICLE

Proof. To calculated the sum of k-Anonymity Accuracy for all levels *h,m,l*:

$$KKA = \frac{Mo(h) + Mo(m) + Mo(l)}{k\ user\ requests\ in\ h + m + l} - (6)$$

These equations, show us how to calculate the query probability in cell and based on that, we can categorized to three of levels: high, medium and low, then compute the entropy as well as the k-Anonymity Accuracy for each cell, then we got the sum of k-Anonymity Accuracy. Obviously, the three of levels gave us of k-Anonymity more than with one level [26] [36], and we have already covered the local map, and the Fgcloak be more effective.

6. CONCLUSION

With the help of entire discussion, new and fine grained spatial cloaking algorithm has been developed. This scheme is capable of guaranteeing the k-anonymity for the mobile users through the provision of fine grained control over the system overhead. Modified Hilbert Curve has been used for the development of FGcloak on the basis of query probability levels for ensuring the protection of the user's privacy.

This scheme further assists in maximizing the cloaking region for the ensuring the provision of improved privacy of the information of mobile users. In this scheme, the query of the mobile user is submitted to the server of location based services with the help of the trusted 3rd party server (for example, location anonymizer). This technique assists in enlarging the queried location into the larger cloaking region as it covers k – 1 other mobile users for achieving the k-anonymity for three levels instead of high level only and we got more of k-anonymity for each cell in the local map. So, we can realized this scheme is most effective Fgcloak with query probability levels.

REFERENCES

[1] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for location-based services," in Proc. of IEEE ICC 2014.
[2] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," in Proc. of IEEE INFOCOM 2011.
[3] J. Krumm, "A survey of computational location privacy," Personal Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009.
[4] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: query processing for location services without compromising privacy," in Proc. of ACM VLDB 2006.
[5] Through spatial and temporal cloaking," in Proc. of ACM MobiSys 2003.
[6] J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: location privacy through camouflage," in Proc. of ACM MobiCom 2009.
[7] B. Niu, X. Zhu, H. Chi, and H. Li, "3plus: Privacy-preserving pseudolocation updating system in location-based services," in Proc. of IEEE WCNC 2013.
[8] J. Manweiler, R. Scudellari, and L. P. Cox, "Smile: Encounter-based trust for mobile social services," in Proc. of ACM CCS 2009.
[9] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in Proc. of IEEE Security and Privacy 2011.
[10] W3C. (2011, Apr.) Platform for privacy preferences (p3p) project. [Online]. Available: http://www.w3.org/P3P/.
[11] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "Cap: A contextaware privacy protection system for location-based services." in Proc. of IEEE ICDCS 2009.
[12] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: privacy-area aware, dummybased location privacy in mobile services," in Proc. of ACM MobiDE 2008.
[13] C.-Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in Proc. of ACM GIS 2006.
[14] L. Sweeney, "k-anonymity: a model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.
[15] I. Bilogrevic, M. Jadliwala, K. Kalkan, J.-P. Hubaux, and I. Aad, "Privacy in mobile computing for location-sharing-based services," in Proc. of ACM PETS 2011.
[16] K. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," Wireless Communications, IEEE, vol. 19, no. 1, pp. 30–39, 2012.
[17] H. Lee, B.-S. Oh, H.-i. Kim, and J. Chang, "Grid-based cloaking area creation scheme supporting continuous location-based services," in Proc. of ACM SAC 2012.
[18] B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 1–18, Jan. 2008.
[19] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," ACM Trans. Database Syst., vol. 34, no. 4, 2009.
[20] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. of IEEE ICPS 2005, 2005, pp. 88 – 97.
[21] C.-Y. Chow, M. F. Mokbel, and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments," Geoinfor-matica, vol. 15, no. 2, pp. 351–380, Apr. 2011.
[22] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in Proc. of IEEE INFOCOM 2014.
[23] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "Mobicache: When k-anonymity meets cache," in Proc. of IEEE GLOBECOM 2013.
[24] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in Proc. of ACM PETS 2003.
[25] Um, J. H., Kim, H. D., & Chang, J. W. (2010, August). An advanced cloaking algorithm using Hilbert curves for anonymous location based service. In Social Computing (SocialCom), 2010 IEEE Second International Conference on (pp. 1093-1098). IEEE.
[26] E. Frejinger, "Route choice analysis: data, models, algorithms and applications," Ph.D. dissertation, Lausanne, 2008.
[27] Niu, B., Li, Q., Zhu, X., & Li, H. (2014, August). A fine-grained spatial cloaking scheme for privacy-aware users in Location-Based Services. In Computer Communication and Networks (ICCCN), 2014 23rd International Conference on (pp. 1-8). IEEE.
[28] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in Proc. of IEEE SECURECOMM 2005.
[29] Z. Xiao, X. Meng and J. Xu, "Quality Aware Privacy Protection for Location based Services," In Proc. of Database Systems for Advanced Applications, vol.4443, (April 2007), 434-446.
[30] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in Proc. of IEEE INFOCOM 2013.

RESEARCH ARTICLE

[31] B. Niu, X. Zhu, X. Lei, W. Zhang, and H. Li, "Eps: Encounter-based privacy-preserving scheme for location-based services," in Proc. of IEEE GLOBECOM 2013.
[32] W3C. (2011, Apr.) Platform for privacy preferences (p3p) project. [Online]. Available: http://www.w3.org/P3P/.
[33] I. Rhee, M. Shin, S. Hong, K. Lee, and S. Chong, "On the levy-walk nature of human mobility," in Proc. of IEEE INFOCOM 2008.
[34] K. Lee, S. Hong, S. J. Kim, I. Rhee, and S. Chong, "Slaw: A new mobility model for human walks," in Proc. of IEEE INFOCOM 2009.
[35] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Mobihide: A mobilea peerto-peer system for anonymous location-based queries," in Proc. of ACM SSTD 2007.
[36] J.-H. Um, H.-D.Kim, and J.-W. Chang, "An advanced cloaking algorithm using Hilbert curves for anonymous location based service," in Proc. 2010 IEEE Second Int. Conf. Social Computing,pp.1093–1098,2010.