# Cyber Security and Privacy-Preserving Analysis for ITSs based on SHF in a continuous query

**Omar Abdulkader[a*], Alwi M. Bamhdi[b], Vijey Thayananthan[a], Kamal Jambi[a], Bandar Al Ghamdi[c]**
[a]Department of Computer Science,King Abdul-Aziz University, Jeddah, KSA
[b]Computer Science College, Umm Al-Qura University, AlQunfodah, KSA
[c]Department of ITC, Arab Open University, Jeddah,KSA

**Abstract**

In the last decade, extensive research related to Cyber Security issues and privacy preserving in Intelligent Transportation Systems (ITSs) and Location Based Service (LBS) have been conducted. The revolution in smart devices, communication, and LBS, encourage users to inquire for their nearest Point of Interest (POI) from LBS providers. This query reveals user's private information such as identity, location, the query context and might be vulnerable to the different type of cyber-attacks. Despite the fact that users are more restricted to protect their privacy against cyber-attacks, they still want to have the maximum benefit from LBS and ITSs, therefore ensuring user privacy will help in LBS pervasiveness. In this paper, we concentrate to provide cyber security and privacy preserving for continuous queries against tracking attacks by adopting clock region with k-anonymity, l-diversity and introducing an efficient and effective discrete technique for continuous query and pseudonym querier in each separate cloak regions. Secure Hash Function (SHF) has been adopted to build the reference between real querier Id and pseudonym. The proposed technique mitigates the computational cost and provides high security and privacy preserving against cyber-attacks.

***Key words:***
*ITSs; Cyber Security; Continuous queries.*

## 1. Introduction

Nowadays with the emergence of the smart devices which become increasingly popular, as those devices embedded with LBSs and Maps applications. In ITSs users can quickly issue a query to inquire for the nearest Gas station, restaurant or ATM. LBSs provider considered user's privacy penetration, as LBSs enforce the users to reveal their actual location when they issue a query. Most of the users want to protect their location privacy, and they refuse to announce their real location. This scenario may cause users to abstain from using LBSs in ITSs. Users are more interested in using LBSs for the service they provided and make it easy to search for a region of interest (ROI) or gathering friend's locations. Therefore, a lot of users are interesting to utilize LBSs and its notice that the number of users using those services are growing rapidly. Consequently, the finest mechanism to preserve the user's private information's and eliminate cyber security issues in ITSs is an urgent need. We also should pay more attention that the pervasive of LBS is restricted by user's confidence. As the users always worry about any issue that relevant to their privacy and sure not want to disclose it, which will cause to limit the LBS pervasiveness. Therefore, we need to have a mechanism to surmounting all cyber security issues relevant to the user's privacy preserving in ITSs.

Several of literature reviews have been proposed a solution for security and privacy preserving in ITSs and LBSs, and most of this proposed mechanism falls under variant approaches, k-anonymity: where the actual user's locations can't distinguish among other users, L-diversity to ensure that there is no homogeneity in released data records. The cloaked region, mix-zone, landmark [1] [2] [3] [4] [5] and private information retrieve: where the querier can retrieve an element from the LBSs data server without the owner of this server can know which element is retrieved [6]. And other adopt the obfuscation and perturbation method to provide the level or privacy preserving. And some of the literature adopt the trust the third-party server to work as a mediator between the querier and LBSs servers. Yong Wang et al. adopt three tire architecture. Based on user's density distributed, history trace and road network topology sent hierarchy was built. Two type of cloaking algorithm for single user and batch of the user were introduced. The proposed model consists of three level: initialization level, where road network hierarchy structure build; Execution level, depending on the precomputed hierarchy structure single users or batch of users will be clocking on Snet if this sub-Snet satisfy users privacy requirements, else. Parent Snet will be considered as clocking region. To maintain the change or modified in the road network. Update level was also introduced to adopt long-term road network conditions. K-anonymity and l-diversity were adopted for cloak single user or batch of users. In their proposed frameworks users could define their security and privacy requirements using users' privacy profile which was adopted for this purpose. By considering users' moving trend, velocity difference, and distance difference, the resilience of proposed framework against typical attack (Homogeneity, query sampling, query replay and tracking attack) was proved.

In [7] several privacy metrics were adopted to protect users' security and privacy to resist against typical attacks. As they

Manuscript received June 5, 2018
Manuscript revised June 20, 2018

adopt k-anonymity and l-diversity in local and global. Which mean if the local area (Snet) as they denoted, is not satisfied predefined users privacy requirements the algorithm will extend to cover global area (Snet). To avoid computational overhead, they define l_max and dis_max as a threshold so, the extended process to cloak querier within Snet will not go to infinite. The proposed model incurs from building road network hierarchy structure; even it's done in the initializing stage. As we know that the road network is vulnerable to frequent modification and changes. Which been handle in the maintenance stage. Consequently, proposed model need for frequent updates.

In continuous queries, queriers are more vulnerable to disclosing their security and locations privacy information among different queries for different locations. The adversary can track\trace users' queries or uses his background to the link between the queries and queriers as the users' identifier remain same in continuous queries.

From this point, and by highlighting in continuous queries, we can conclude that if we have the mechanism that eliminates adversary ability to infer any relevant information from continuous queries. In this case, we will be able to contribute in the felid of knowledge (cyber security and privacy-preserving) regarding discrete continuous queries spatial\temporal interval and pseudonym queriers for each interval aiming to destroy adversary ability to track\trace or using its background knowledge for link purpose.

The proposed model divides into three phase; discrete queries into spatial\temporal intervals, queriers' pseudonym in each spatial\temporal intervals and building hash table to manage and control the pseudonym with main Ids. Consequently, our contributions in on this paper can be summarized as follows:

- Discrete-continuous queries into spatial\temporal queries. In continuous queries, as queriers are related to different spatial\temporal intervals, still their identifier remains the same in all intervals which make it an easy task for the adversary to infer sensitive information or disclose querier real locations by track\trace or linking among continuous queries. Therefore, in our contribution, we aim to eliminate the adversary ability to track\trace or link ability by pseudonym the querier at different spatial\temporal intervals, this will provide a level of cyber security and privacy for the queriers.
- Pseudo each discrete queries with a different identity. So, it will be impossible for the adversary to infer any information about querier by tracking those queries or using background knowledge.
- Cloak each discrete queries to ensure that queriers are anonymized among other users within same cloak region. Also, ensure that there is no leak of diversity that leads the adversary to link between a query and certain user.
- Adopting Secure Hash Function to build reference table that handles, maintain and control the main queriers' identifier and their pseudonym.
- Build refine engine to refine the retrieved results from LBS server. And return the refined results to the queriers.

The rest of the paper is organizing as follows. Section 2 discusses the literature review and related works on cyber security and privacy-preserving domain. The proposed methods are discussing in section 3. Experimental results are highlighted in section 4. Section 5 discusses the system evaluation. Finally, the paper concludes in section 6.

## 2. Related Work

Massive of researches have been conducted and published on ITSs, LBS, Cyber security, and privacy preserving. Literature review on this domain are variant and different solutions have also been proposed to address cyber security and privacy issues. Yaqing Shi [8] et al. works on two adjacent points and considering the uncertainty between those points to provide more accurate CRQ, they proposed a CPRQP algorithm based on Hadoop firstly. Sergio Mascetti [9] et al. proposed a proximity service, when a friend (called buddies) want to contact to each other through proximity service (friend finder) while preserving their location privacy from the untrusted service provider. They are not considering the anonymity because they assume that the involve users supposed to know each other. Malladu Madhulatha [10] et al. and Krishna Puttaswamy [11] et el. LocX (short for a location to index mapping) application has been proposed, the main idea is to transfer the location coordinate, and this transformer formula considers as a secret between social groups. Also, they provide transformer formula for both point queries and KNN queries. They adopt cloud as untrusted third party server. Consequentially they use location coordinate transformer formula. They use AES with 128 bits' keys for encryption and decryption.

Doohee Song [12] et al. proposed anonymity of motion vector (AMV) to provide anonymity within the cloaked region that ensures the querier is indistinguishable among K users within the cloaked region. AMC consist of the centralized LBS server, the location anonymizer, and the client. Dario Freni [13] et al. address privacy preserving related to social network resources when users publish a resource that contains spatial and temporal tags. They proposed a technique to provide privacy for two scenarios, location privacy, and absence privacy. The former related to reveal any information about the availability of the user in a specific location at given time and the latter mean that the user is not in a specific location for a given time. In [14] Yuqing Sun et al. introduce a secure path notion based on series of privacy metrics such as distance and QoS. The key factor behind this idea is that they are trying to recommend a secure path for the user's movement instead of or tracing his path and avoid the burden of calculating the cloaked region to provide a level of k-anonymity.

In [15] they proposed a mechanism for two level of anonymity first ensure that the querier is anonymity within his segment. Then they go further to anonymize the segment with another segment nearest to querier segment. Also, introduced the notion of reciprocal. It's obviously suffering from computational overhead. Russell Paulet [16] et al. they introduce privacy preserving in LBS by adopting private information retrieval. Their proposed approach consists of two-stage: in the first stage, they adopt transfer techniques and associate symmetric key, while the second stage the communication between user and server is done with PIR. The retrieved results are encrypted. Therefore, the user will decrypt using the symmetric key which has been associated with the first stage. Their model consists of three tire architecture by adopting trusted 3rd party. They proposed EPQ scheme. In their proposed scheme they adopt a cloud server as an untrusted server to store encrypted data. The scenario is as follow: LBSs has the location data. So, those data are encrypted by LBSs and send it to cloud server. Also, LBS compute the data set and upload it to a cloud server to perfume privacy preserving. Before users issue a query, he should register to LBS. after the registration process users can issue a query to cloud server. Then cloud severe authenticate user's registration after that they provide the users with encrypted data. Users collect the key from LBS; then he decrypts the data to get exact locations [17].

In [18] they adopt k-anonymity notion by define user's privacy profile. A special generalization algorithm has been developed to cloak regions that meet user's privacy requirements. Chien-Ping Wu [19] et al. proposed split up the cloaked algorithm based on k-anonymity notion. In their proposed methods they give the users the chance to define the privacy requirements. Upon those requirements, they split up the cloaked region to meet user's requirements trying to make the cloaked region small as much as they can. Also, they adopt the concept of local and global anonymity. In [20] they proposed a (PCQP) short for private circular query protocol, the proposed protocol consist of two-phase: firstly, they connect user's point of interest (POI) using Moore curve. In this phase circular structure has been formed from those POI. Second phase pallier cryptosystem has been applied to encrypt the related information to a circular structure which has been formed in the first phase.

Haibo Hu [21] et al. demonstrated and showed that they could provide privacy preserving for the query result authentication without disclosing the actual location or any relevant information of the data owner. In [22] they proposed DUMMY-Q as a novel solution for query privacy-preserving, as they are going to issue dummy queries along with the real query. As they work on continuous queries. Therefore, querier movements are considered. In [23], they proposed a hybrid K-NN algorithm which consists of two methods, to blur user's real location and provide k-anonymity. Firstly, they adopt cloaked region, in the second level they encrypt the query by adopting private information retrieval (PIR). The enhancement in their approach, by cloaking region and adopt PIR they only consider the cloaked region instead of looking for the whole database in LBS server. To improve the performance of PIR, MSQL and NSQL have been proposed, as an efficient and effective schemes for storing and organization of POI location. In their proposed scheme, secure HW (secure coprocessor) has been considered as trust mediator between users and LBS server. The experimental results show that multi-layer flexible mesh technique is more effective for reducing PIR when query location is close to the highly dense cells [24].

Roman Schlegel [25] et al. proposed a dynamic grid system, where the users have the ability to define their privacy requirements as they named query area. Then based on dynamic grid structure the query area divided into an equal-sized grid cell, then those two (query information and grid identity) are encrypted and sent to the semi-trusted query server, which in turn forward to the service provider to decrypt and returned results. Kamenyi Domenic M [26] et al. propose three tire architecture method that consists of the client, trust-but-curious server, and LBS server. Trust server itself consists of two components. Mixing Engine, which adopts mix-zone and introduced two algorithms. OMLS that optimize mix-zone placement. SBGA to satisfy users predefined privacy requirements. And Result Refiner, which to refine the returned results. In [27] PIR has been adopting to provide privacy preserving for short path queries. Hardware-aided called Secure Co-processor (SCP) had been implemented as a mediator between querier and LBS dataset. Finally, Yiming Wang [28] et al. adopt cloaking region to achieve user's privacy preserving. They go beyond normal clocking methods to include the speed and heading direction to avoid different scenarios of inference attacks.

## 3. Proposed System Model

Our proposed system model falls under three-tier architecture. Figure (1): shows system architecture which consists of three components ;( 1) Client: the users who issue the queries. (2) Trust third-party anonymizing server (TAS): which locate as a mediator between the client and LBS server in ITSs. We assume that the channel between the client and the TAS is a secure channel. Therefore, how to secure this channel is beyond this paper. (3) Finally, the LBS server which contains POI database. Most of the literature review which applied for road network are incur from building the road networks topological either using their method to create the mapping to the road network or by adopting Voronoi network diagram. Despite, the building or establishing the road network mapping is done in the initializing stage. It still incurs from the computational overhead. In our paper, we assume that the moving objects are laid on the road network. Consequently, when the user issue query in the form of (Uid, L, P, Cont) where Uid is the User identifier, L: Real User location, P: refer to the user privacy profile, where Cont: refer to the query context, with his/her real location (as we assume user's location lay within the road network) from this real location we search for the nearest neighbor. After we determine the nearest object to the querier. We draw the line between them. This line (R) will consider as the circle radius. The process of creating cloak region querier anonymizing will be discussed in the subsection B.

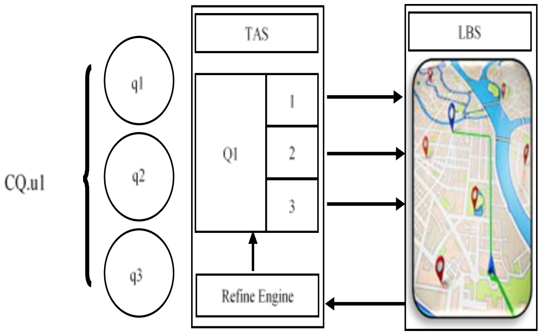


Fig. 1 System architecture

## A. Discrete Continuous Queries

The main contribution in our proposed model is that discrete Continues Queries (CQ). The querier issue a query searching for a his\her point of interest (POI) in the form (Uid, L, P, Cont) as an example: (give the nearest ATM for the next 12km). We consider this query as spatial continuous query where user interesting to retrieve the nearest ATMs for the next 12 KM. Therefore, we discrete the query from spatial aspect into three queries where each query contains only 4 km as shown in figure (3). Also, we will create a separate cloak region for each query and pseudonym the querier in each discrete query. Consequently, up to this level and by discrete and pseudonym the querier, we achieve two goals, first: in each cloaked region users (queriers) are not distinguishable among other users within same cloaked regions. Second: by change user's identifier in each cloaked region the adversary is not able to track\trace the queriers or by the correlation between continuous queries. Those two goals provide a level of a cyber-security based on anonymity and user's LBS. Table (1): show that two queriers (Q1 and Q2) where the queriers are cloaked in three different cloaked regions as shown in the table (1) the querier id for Q1 is O24, and the pseudonym within next cloaked region are O24-1 and O24-2 respectively. R is referring to the circle radius for each cloak regions. Objects within cloaked regions refer the quantum of the objects that queriers are anonymized among them. We notice that there are some recur objects in different cloak regions which mean that there are some objects which are moving with the same trend of the querier. In CR1, CR2 and CR3 we notice that (O97) recurs. Same for the (O16) which recur in two different cloak regions (CR2 and CR3). Table (1) also show the result for the querier 2.

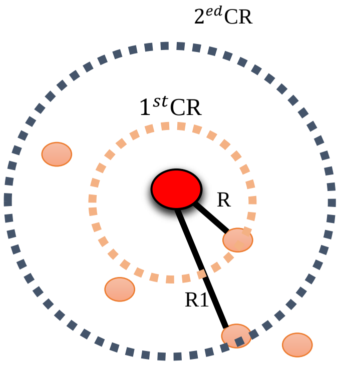


Fig. 2 The process for crate the cloaked region.

## B. Cloak Regions and Anonymize Process:

Table 1: Querier, cloaked regions and pseudonym

| Querier | CR | Object ID | R | Objects in CR |
|---|---|---|---|---|
| Q1 | CR1 | O24 | 4452 | O3 O38 O97 O25 |
| | CR2 | O24-1 | 4466 | O48 O97 O18 O16 |
| | CR3 | O24-2 | 5408 | O97 O16 O1 O9 |
| Q2 | CR1 | O27 | 5953 | O62 O58 O22 O24 |
| | CR2 | O27-1 | 6716 | O58 O24 O62 O5 |
| | CR3 | O27-2 | 5071 | O16 O58 O48 O9 |

As aforementioned, the querier sends his\her real location while issuing the query. Starting for this real location which contains (x, y) coordinate, we go further to search for the nearest neighbor using KNN algorithm. After we determine the nearest object. We draw the line between the querier and the nearest object. We define this line as R which refer to the circle radius. Using the value of R, we will draw the circle. This circle will be the first cloaked region. Within this circle, we will search for the objects which are lay inside the circle or on circle borders. With user privacy profile, the querier can specify his\her privacy requirements. Therefore, when we search for the objects inside the circle we check the user requirements in the user privacy profile, if the quantum of the objects inside the circle satisfies the predefined user privacy, we considered the circle as our clocked region. Otherwise, we research for the next nearest neighbor to the querier, after we found this object. We follow the steps mentioned above to create the new clocked region that satisfies user privacy profile requirements. Figure (2) shows the process of creating the clocked region and anonymize querier among other users within the circle.

## C. Pseudonym (querier Identifier):

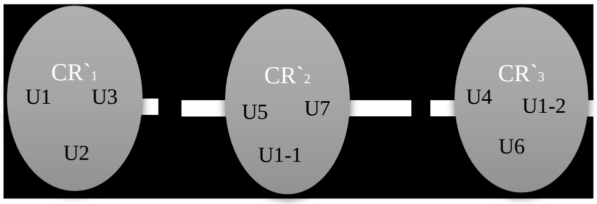


Fig. 3 Creating cloaked regions for the querier.

The adversary ability to track\trace queriers increased in continuous queries. Previous contributions considered only to anonymize the queriers with cloak region but they did consider to pseudonym the queriers identifier as it remains the same identifiers at different spatial\temporal intervals. Our proposed model aims to change the querier identifiers in each spatial\temporal interval. Figure (3) shows three cloak region CR1, CR2, and CR3 on the road networks; our proposed model aims to pseudonym U1 in CR2 and CR3. Therefore, U1 appears in CR2 and CR3 as U1-1 and U1-2 respectively.

## D. Building Reference table

To manage the querier's identifiers and their pseudonym, we build reference table using a hash function as it provides security data access and most comfortable in implementation. Also, to ensure that the identifier references are not tampered with while transmitted among trusted third party server and LBSs.

## E. Attacks model:

Attack model can be divided into two types; background knowledge and typical attacks, where typical attacks divided further into four types; Homogeneity, query sampling, query replaying and tracking attack. We will discuss those type in details within next sub sections.

1) Background knowledge.

Adversary background knowledge about querier or queries context may guide him to infer some sensitive or privacy information if he collects any pace of information from the queries context such as User Id, real location, regions of interest. As he will be able to correlate any gathering information’s with his background knowledge about the users.

2) Typical Attack.

Several contributions have been proposed to resist those type of attacks. Our proposed model proved its ability to resist against those types of attacks, as it shown in experiments and results evaluation. Within next subsection, we will discuss those typical attack.

a) Homogeneity.

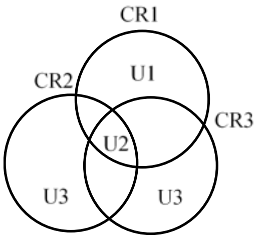


Fig. 4 Misdistribution of user’s locations (query sampling).

K-anonymity consider as promising techniques that blur users among other users in the same region. However, it still vulnerable to different attacks. L-diversity appears to overcome the shortcoming in k-anonymity and has the ability to works as a firewall that prevents the adversary infer any sensitive information by using his background knowledge as links to infer or conduct any sensitive or privacy information from queries context. And ensure that there is no leak diversity in the released database records.

b) Query sampling.

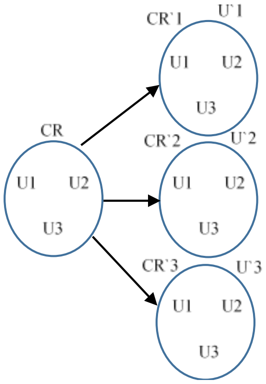


Fig. 5 Show how adversary replaying the query to infer querier.

This type to attack refer to the adversary ability to link the queries to the querier using his background knowledge. Due some misdistribution of the queriers as some cloak regions are overlapped, and the same querier appears in different clock region. Therefore, the adversary can easily disclose querier for this query. Figure (4) show that U1 appears only in CR1 while U2 and U3 appear in both CR2 and CR3. Consequently, U1 is vulnerable to be easily disclosed. In this case and to eliminate adversary ability to disclose the querier using query sampling, our proposed model aims to tackle this type to attack through ensuring there are well distributed for querier in different overlapping location and identifiers.

c) Query replay

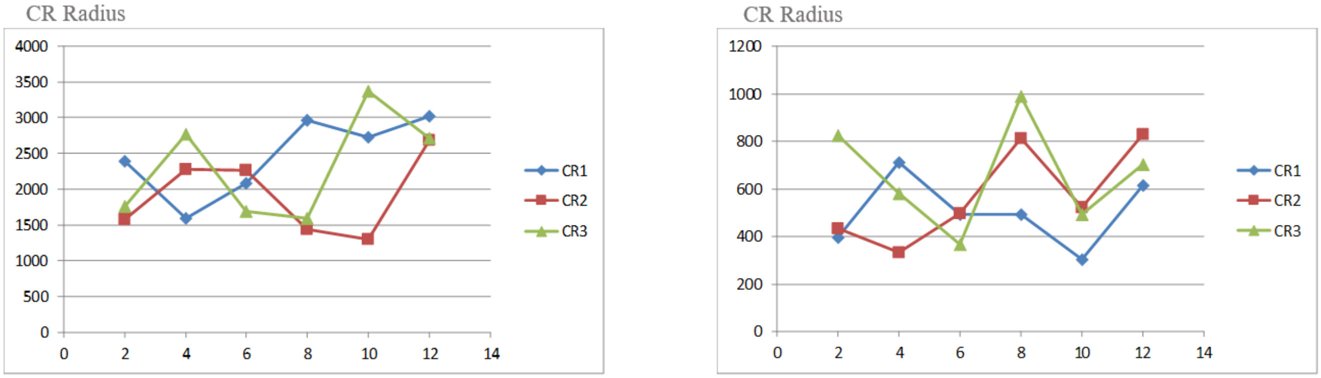
In this type of attack, the adversary tries to replay the cloaked region. Figure (5): describe how the adversary is replaying the query. Let consider the cloaked region (CR) which contain three users (U1, U2, and U3) is the cloaked region for our proposed model. To replay and infer which user is the querier. Adversary creates three cloaked regions by assuming different querier in each created cloak region, U`1, U`2 and U`3 for CR`1, CR`2 and CR`3 respectively. Then the adversary calculates the probability for each user and considers the highest probability as the querier. In our proposed model, the adversary unable to replay the query due to the level of k-anonymity, l-diversity, and pseudonym hypothesis.

d) Query tracking

This paper is more concentrate on tracking attacks and the proposed model ensure that the adversary ability to track or infer any information from the continuous queries or any relevant information to the queries are eliminated.

## 4. Experiments and Results Evaluation

As we are aiming to provide privacy preserving for the continuous queries by adopting discrete\burst notion, this section evaluates our model by conducting several experiments and compute the average results. Most of the proposed techniques for privacy preserving in road networks incur from the building road network hierarchy some by adopting network Voronoi diagram (NVD) and other by their mechanism. In our proposed model we assume that the querier and candidate moving objects are within road network topological. Consequently, the user coordinate which determines the his\her actual location that associate with the query lay on road networks. Also, the candidate objects nearest to the querier are within road networks frontier. That what makes our proposed model fast computation, more efficient and more effective. We evaluate the proposed model based on the following aspects:



(A): work area 50X50 No. of Objects 500.

(B): work area 50X50 No. of Objects 1000.

Fig. 6 Cloaked regions volume with same work area and different No. of objects. Radius are calculated in M.

Table 2: Queriers pseudonym process and discrete continuous queries example to create cloaked regions.

| Queries | Objects ID | CR. Radius | Objects within CR |
|---|---|---|---|
| Q1 | O6911 | 85 | O69404 O80185 O96416 O76360 |
| | O6911-1 | 89 | O51727 O80185 O59765 O58858 |
| | O6911-2 | 117 | O80185 O6955 O50238 O49918 |
| Q2 | O13882 | 72 | O36160 O30165 O49465 O27425 |
| | O13882-1 | 55 | O10604 O77082 O72534 O36160 |
| | O13882-2 | 142 | O36160 O87704 O81912 O61416 |

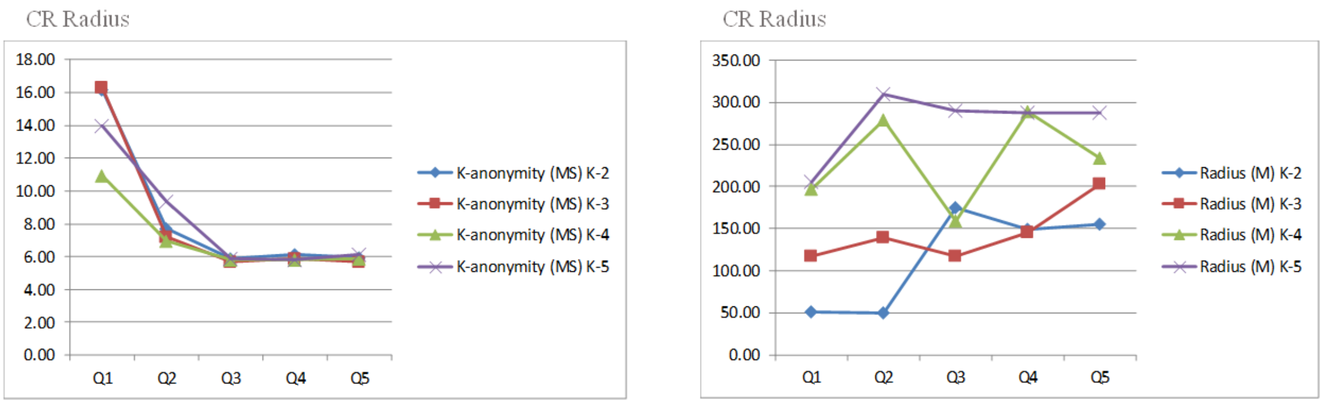
### A. Discrete metrics:

Table 3: The average for cloaked regions cost with variant predefined k-anonymity values. Cloaked regions cost calculated in MS.

| Oid | K-anonymity (MS) | | | |
|---|---|---|---|---|
| | K-2 | K-3 | K-4 | K-5 |
| Q1 | 16.17 | 16.31 | 10.94 | 13.97 |
| Q2 | 7.75 | 7.23 | 6.96 | 9.37 |
| Q3 | 5.87 | 5.70 | 5.81 | 5.86 |
| Q4 | 6.13 | 5.89 | 5.81 | 5.81 |
| Q5 | 5.93 | 5.72 | 5.87 | 6.14 |

Using discrete for continuous queries aim to provide privacy preserving to the querier identifier. Therefore, by discrete queries into separate spatial\temporal intervals and pseudonym quartier's identifier in each separate interval will hide the user's Id. Adversary tracking\tracing ability will be eliminated as the querier Ids are different in each cloak regions. This can be considered as one of our main contributions in this paper. After change queriers Ids, we need to build a table that manages and reference queriers sub Id to the main ID. Therefore, we adopt hash function. The experiment results show that proposed model dose does not incur computational overhead. Table (2) shows the queriers main Ids, sub Ids and the candidate objects within different cloaked regions.

## B. Creating cloak region cost:



(A): Work area 10X10 No. of Objects 2000.

(B): Work area 10X10 No. of Objects 2000.

Fig. 7 Cloaked regions creation cost with same work area and same No. of objects with variant predefined k-anonymity values (2-5). Creation cost calculated in MS, where Radius are calculated in M.

We conduct our model with a different scenario to observe, infer and analyze different results. As aforementioned in our model querier defined his\her privacy that satisfies his privacy requirements. Therefore, the cloak region size and radius are partially correlated to the predefined k-anonymity value. Table (3) shows how the cloak region creation cost is related to the predefined k-anonymity values.

Table 4: The average for cloaked regions volume with variant predefined k-anonymity values. CRR calculated in M.

| Oid | Radius (M) | | | |
|---|---|---|---|---|
| | K-2 | K-3 | K-4 | K-5 |
| Q1 | 51.33 | 116.67 | 196.33 | 205.33 |
| Q2 | 50.33 | 138.67 | 278.33 | 309.33 |
| Q3 | 175.00 | 117.67 | 158.67 | 290.00 |
| Q4 | 148.67 | 145.00 | 288.33 | 287.00 |
| Q5 | 155.67 | 202.33 | 233.67 | 287.33 |

## C. Privacy achieving:

Users can define their privacy requirements. Therefore, when queriers issue continuous queries, they can specify the degree of privacy which reflects user's severity and desire of privacy preserving. Among this predefined anonymizing value as shown in the table (4). Our proposed model creates the cloaked regions that satisfied queriers' anonymizing requirements. Cloak region creation cost and radius size correlate to the anonymizing values and objects distributed in the work area. Our proposed model implemented to create cloak regions with minimum size as much as it can, which reflect the QoS for the proposed model. Figure (6): shows the effect of the objects distributed within the work area. Thus, as the number of objects is increased and the objects distributed are closed to each other, this will produce a small size of cloak region.

## D. Experiment setup:

Table 5: Experiment parameters.

| Parameters | Value | Unit |
|---|---|---|
| Work area | 10X10, 20X20 and 50X50 | Km |
| Number of Objects | 1000 – 100,000 | - |
| Privacy (k-anonymity) | 2-8 | - |
| Distance | 2,4,6,8,10,12 | Km |

We implement our simulation using JAVA; the experiment conducts on DELL Laptop with following specifications: Intel CORE i5 vPro. 8GB RAM. Window 7 X 64 Enterprise operating system. The simulation runs several times with a variant scenario to calculate the average values for different parameters. Simulation has been conducted with varying areas of work (10X10, 20X20 and 50X50) km. Some objects are variant between 2000 – 100,000 objects. The simulation shows that when a massive number of objects distributed within a small area will produce to have small cloak region, as the objects lie close to each other, which mean that the querier predefined k-anonymity to blurs the querier among other nearest objects will be achieved with low radius values and vice versa. Table (5) shows the experiment parameters.

### E. Experiment results:

Figure (6): shows the effect of number of candidate objects within the same area figure (a) 500 candidate objects moving in 50X50 work area size and the privacy-preserving region between (1300 - 3400) while figure (b) 1000 candidate objects moving in the same size of work area and the privacy-preserving regions between (300 - 1000). Based on that we conclude that the size of work area, quantum of the candidate objects and their distributed density considered as main factors that affect the size of the privacy-preserving region.

Figure (7): shows the relation between cloaked regions and variant predefined k-anonymity values in both creation costs and radius size. From figure (a) and (b) we conclude that cloak regions creation cost and radius size are increasing gradually as the k-anonymity values increased. Also, we should pay more attention to the querier surrounding objects within road networks, this factor is considered as an important key factor that effects on the cloaked regions radius size and creation costs as well. Also, from the figure, we notice that if the objects distributed within road network are closed to each other, this will lead to having small cloaked regions which consider like the quality of service for our proposed model.

## 5. Conclusion and Future Work

Recently, cyber security and privacy-preserving for the continuous query in ITSs and LBS have been gained a lot of researchers interesting, and tremendous of contributions also have been published in this domain. Most of the contributions either based on trusted third-party server or non-based. In the proposed model k-anonymity, l-diversity, and cloak regions have been adopted to provide security and privacy preserving for queriers. Discretion the continuous queries into spatial\temporal intervals and pseudonym each interval with different identifiers eliminate the adversary ability to track\trace the queriers. In our approach queries can define their own privacy degree based on variant circumstances. Also, cloak regions creation cost has been minimized significantly comparing with other models. Up to our knowledge, this is the first paper that adopts the discrete and pseudonym quriers. Previous works rely on cloaking users to different locations, however, user's IDs remain the same. Our novel approach shows its efficiency to resist tracking\tracing attacks, as the user's identifier change in each different points of cloak regions in the continuous queries. Consequently, adversary tracking ability has been eliminated. Several experiments show that the cloaked regions creation cost and radius size are affected by several factors such as work area size, some objects within the work area, predefined k-anonymity, and objects distributed within this work area. For future work, we aim to adopt the notion of Land Mark with our proposed model. By adopting landmarks, we hope that the process of clocking queriers will be more efficient and effective. As those Land Marks will be considered as cloak regions for the queriers and it's calculated in the initialize phase of the proposed model. Obviously, this will reduce the computational overhead and the cost of creating cloak regions. As this paper only considers to pseudonym only the queriers, further we may also consider to pseudonym the candidate object that recurs in spatial\temporal intervals.

## References

[1] Zhou Shao, David Taniar, Kiki Maulana Adhinugraha, "Range-kNN queries with privacy protection in a mobile environment," Pervasive and Mobile omputing, elsevier, 2015.

[2] Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux, "On the Optimal Placement of Mix Zones ," Springer-Verlag Berlin Heidelberg, 2009.

[3] Balaji Palanisamy, Ling Liu, Kisung Lee, Aameek Singh and Yuzhe Tang, "Location Privacy with Road network Mix-zones,".

[4] Balaji Palanisamy, Sindhuja Ravichandran, Ling Liu, Binh Han, Kisung Lee and Calton Pu, "Road Network Mix-zones for Anonymous Location Based Services,".

[5] Amirreza Masoumzadeh_, James Joshi, "Top Location Anonymization for Geosocial Network Datasets," TRANSACTIONS ON DATA PRIVACY, 2013.

[6] Roopa Vishwanathan, Yan Huang, "A Two-level Protocol to Answer Private Location-based Queries," IEEE, 2009.

[7] YongWang a, YunXia a, JieHou a, Shi-mengGao a, XiaoNie a, QiWang, "A fast privacy-preserving framework for continuous location-based queries in road networks," Journal of Network and Computer Applications,elsevier, 2015.

[8] Yaqing Shi ,Jun Feng and Zhixian Tang, "UPBI: An Efficient Index for Continues Probabilistic Range Query of Moving Objects on Road Network," International Journal of Multimedia and Ubiquitous Engineering, 2015.

[9] Sergio Mascetti _ Dario Freni _ Claudio Bettini _ X. Sean Wang _ Sushil Jajodia, "Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies ," arXiv:1007.0408v2 [cs.DB] 6 Nov 2010.

[10] Malladu Madhulatha, V. N. V. Revanth Kuma," Preserving Location Privacy in Geo-social Applications for Server Maintenance," International Journal of Innovative Technologies, june-2015.

[11] Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer,Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao, "Preserving Location Privacy in Geo-Social Applications," IEEE TRANSACTIONS ON MOBILE COMPUTING, 2012.

[12] Doohee Song, Jongwon Sim, Kwangjin Park and Moonbae Song, "A Privacy-Preserving Continuous Location Monitoring System for Location-Based Services ," International Journal of Distributed Sensor Networks,2015

[13] Freni1 Carmen Ruiz Vicente2 Sergio Mascetti1 Claudio Bettini1 Christian S. Jensen, "Preserving Location and Absence Privacy in Geo-Social Networks," CIKM'10, October 26–30, 2010.

[14] Yuqing Sun, Haoran Xu, Reynold Cheng, “Privacy Preserving Path Recommendation for Moving User on Location Based Service ,” IEEE 10th International Conference on Ubiquitous Intelligence & Computing, 2013.
[15] Wei Li, Jiangtao Jiang, Yunchun Li, GuoJun Li, “A Query-Aware Location Privacy Protection Approach in LBS for Road Networks,” IEEE International Conference on Green Computing and Communications, 2013.
[16] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, “Privacy-Preserving and Content-Protecting Location Based Queries ,” IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, MAY 2014.
[17] Hui Zhu, Rongxing Lu, Cheng Huang, Le Chen, and Hui Li,” An Efficient Privacy-Preserving Location Based Services Query Scheme in Outsourced Cloud,” IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2015.
[18] Xihui Chen, Jun Pang, “Measuring Query Privacy in Location-Based Services,” CODASPY’12, February 7–9, 2012.
[19] Chien-Ping Wu, Chen-Che Huang, and liun-Long Huang, Chib-Lin Hu, “On Preserving Location Privacy in Mobile Environments ,” The 7th International Workshop on Mobile Peer-to-Peer Computing, IEEE, 2011.
[20] Ting Lien, Yu-Hsun Lin, Student Member, IEEE, Jyh-Ren Shieh, and Ja-Ling Wu, Fellow, IEEE, “A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift for -NN Search ,” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, JUNE 2013.
[21] Haibo Hu, Qian Chen, Jianliang Xu, “VERDICT: Privacy-Preserving Authentication of Range Queries in Location-based Services ,” IEEE, 2013.
[22] Aniket Pingley∗, Nan Zhang∗, Xinwen Fu †, Hyeong-Ah Choi∗, Suresh Subramaniam∗, and Wei Zhao, “Protection of Query Privacy for Continuous Location Based Services,” IEEE, 2011.
[23] Mi Young Jang, Sung-Jae Jang, Jae- Woo Chang, “A new K-NN Query Processing Algorithm Enhancing Privacy protection in location-based Services,” IEEE First International Conference on Mobile Services, 2012.
[24] Shyue-Liang Wang1, Chung-Yi Chen1, I-Hsien Ting1 and Tzung-Pei Hong, “Multi-layer Partition for Query Location Anonymization,” IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012.
[25] Roman Schlegel, Chi-Yin Chow, Qiong Huang, and Duncan S. Wong, “User-Defined Privacy Grid System for Continuous Location-Based Services,” IEEE TRANSACTIONS ON MOBILE COMPUTING, OCTOBER 2015.
[26] Kamenyi Domenic M., Yong Wang, Fengli Zhang, Imran Memon, Yankson H. Gustav, Preserving Users’ Privacy for Continuous Query Services in Road Networks, 6th International Conference on Information Management, Innovation
[27] Kyriakos Mouratidis, “Strong Location Privacy: A Case Study on Shortest Path Queries,” IEEE, 2013.
[28] Yiming Wang, Lingyu Wang and Benjamin C. M. Fung, “Preserving Privacy for Location-Based Services with Continuous Queries ,” IEEE, 2009.