Improving the Performance of kNN Queries with Location Privacy

Raed Al-Dhubhani
Department of Computer Science
College of Computing and Information Technology
King Abdul-Aziz University, Jeddah, KSA
Email: r.aldhubhani [AT] stu.kau.edu.sa

Jonathan Cazalas
Department of Computer Science
College of Computing and Information Technology
King Abdul-Aziz University, Jeddah, KSA

Abstract— **With the big growth in the number of mobile devices worldwide, providing services to the mobile users represents a big market. Location Based Services (LBSs) provides the mobile user with valuable and rich information about his surrounding based on his location, which is very helpful in the activities of his daily life. Using these valuable services introduces the threat of the unauthorized access to the user location data. Location privacy is an important issue in mobile computing field, where revealing the accurate location of the LBS user is not only revealing his longitude and latitude values, but it goes beyond that to be used to analyze these values to infer sensitive information about his life style activities. In this paper, we are aiming to improve the efficiency of the location privacy technique which is based on the Paillier public-key cryptosystem. The objective is to improve the performance by reducing the communication cost. Experiments have shown that the communication cost is reduced up to 39.4 %.**

Keywords- k Nearest Neighbor (kNN), Location Based Services (LBS), Location privacy, Mobile Computing.

I. Introduction

Increasing the number of mobile devices worldwide leads to emerge new type of services which were especially developed for this type of devices. In addition to that, embedding the GPS units for most of these mobile devices leads to the growth in the market of services which depends on the user location. Recently, mobile users depends more on the Location Based Services (LBS) for their importance for the different life aspects. By using these services, users can allocate restaurants, coffee shops, shopping malls, hospitals, and even the existence of their relatives and friends in their surroundings. Some LBSs also enable the users to write notes, and descriptions, link them to specific locations, and share these notes and descriptions with others.

According to [1], the global revenue of the global LBS market is expected to grow more than 300% in comparison to 2010 as shown in Fig. 1. The main factors of this growth in the LBS market are: the increase in the GPS-enabled smartphones, the growth of mobile advertising, and the improvement in the coverage and speed of mobile networks [1]. The success of LBSs depends on their ability to provide accurate information which depends on using the accurate location of the user. On the other hand, LBS users are concern on keeping their location privacy. Most LBS users are not comfortable with the potential revealing to their accurate locations to untrusted parties, which leads to misuse this valuable data.

Location privacy is an important issue in mobile computing field. Revealing the accurate location of the LBS user may be used to get further information. Analyzing the data of the user's location may lead to infer sensitive information about his life style activities, habits, political direction, religion, and even more. According to [2], it is not necessary that LBS provider is considered as the untrusted party who wants to misuse the location data of the user. In contrast, LBS provider servers could be compromised by a third party (the adversary) in order to access the data of the user location. Hence, providing the location privacy of the LBS user is also important for LBS providers, because it ensure that the users of their provided services trust and feel comfortable to use these services, and then ensure the investments feasibility of the LBS providers. So, the goal is how to enable the user to use the provided LBSs and at the same time protect his location privacy.

There are many techniques which have been used to provide the location privacy. Information Access Control technique [3], [4] is one of these techniques which depends on the LBS provider to have a mechanism to control the access of the users' location data. This technique is vulnerable to the misbehavior of the LBS provider. Mix Zone [5] is another technique which depends on introducing an intermediate server to anonymize the user location. The drawback of this technique is the vulnerability of the intermediate server to be compromised by the adversaries. K-anonymity [6], [7], [8], [9] is applied by grouping the mobile users in groups of k members and constructing the group bounding region. Then, each user uses the bounding region of his group to send the queries to the LBS provider. Using an intermediate server to group the mobile users makes it vulnerable to be compromised by the adversaries. Dummy locations [10], [11], [12], [13] depends on confusing the LBS server about the real location of the object by sending the same query of the mobile users many times with different location values, where all these location values are faked and randomly generated except one which represents his real location. Using random locations to cover the real location of the user is the weakness of this technique where the patterns of the user locations received by the LBS server can be analyzed to infer his real location. Geographic data transformation [14], [15], [16], [17] is based on transforming the user data using a secret transformation key, and hosting the transformed data in the LBS server. To access this data, the user secret key is needed to retrieve the original data. Analyzing the access patterns of the LBS services can lead to infer the user transformed locations data, because the same query returns the same encoded location. Private Information Retrieval (PIR) [18], [19], [20], [21], [22], [23] depends on using cryptography systems to provide the location privacy. Building special hardware for this purpose and embedding the secret keys to the hardware by the manufacturer is vulnerable to the misbehavior of the hardware manufacturer.

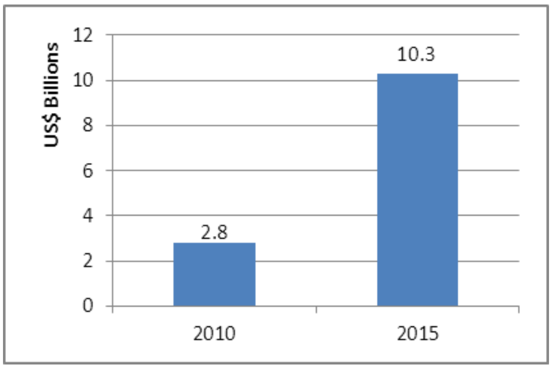

Fig. 1: Revenue Expectation of Global LBS Market

In [24], location privacy technique has been introduced which is based on Paillier public-key cryptosystem [25]. The technique has three stages: query generation, response generation and response retrieval. In the query generation stage, the clocking region is constructed as n*n cells, while the columns flags represent indicators to the existence of the user in the columns of the cloaking region. To generate the response, the LBS server uses the encrypted column flag sent by the mobile user to generate the kNN vector of each cell in the cloaking region. In the response retrieval stage, the mobile user retrieves the query result by decrypting the values received from the LBS server using the secret key of the mobile user. Calculating the kNN vector of the center of each cell and then using that kNN vector for all the points located inside that cell affects the accuracy of the kNN query. Improving the query accuracy is implemented by querying the kNN vectors of the neighbor cells of the current cell of the mobile user. So, the authors suggest querying one or three more kNN vectors of the neighbor cells.

In this paper, the aim is to improve the performance of the location privacy technique which is based on the Paillier public-key cryptosystem.

So, our contribution is based on the following two points:

1) Reducing the communication cost which results from querying the additional neighbor cells by reducing the number of these additional queries.

2) Improving the accuracy of the kNN queries for cells with large size by querying the four sub-cell centers of the cell 'Looking Inside' instead of querying the neighbor cells of the cell 'Looking Outside'.

The remainder of the paper is organized as follows. Related works to the location privacy are discussed in Section II. Section III describes our contribution in more details. The evaluation of our contribution and the experiments setup, parameters and results are shown in Section IV. Section V contains the conclusions and future work of the paper.

II. RELATED WORK

In this section, the techniques which have been developed to provide the location privacy are discussed.

Information Access Control [3], [4]: In this technique, the assumption is that the LBS provider has a mechanism to control the access of the users' location data. This involves building and implementing policies to control the access to the users' location data. The problem of this technique is classifying the LBS provider in the security model of the LBS location privacy as the potential adversary who may misuse the location data of the users.

Mix Zone [5], [26]: Mix zone is another location privacy technique which depends on introducing an intermediate server to anonymize the user location. So, when the mobile user enters a mix zone, the intermediate server assigns a pseudonym to him. And then the user uses that pseudonym to send his query to the LBS server via the intermediate server. When the mix zone of the mobile user is changed, a new pseudonym is assigned to him. Mix zone technique is currently used for road networks. The drawback of this technique is the vulnerability of the intermediate server to be compromised by the adversaries.

K-anonymity [6], [7], [8], [9]: This technique is applied by grouping the mobile users in groups of k members. And then a bounding region is constructed for each group. Then, each user uses the bounding region of his group to send the queries to the LBS provider. An intermediate server is required to construct the bounding region of the users. For the adversary, the location of the user can be identified with a probability not higher than 1/k. This technique is also has the same drawback of compromising the intermediate server by the adversaries.

Dummy locations [10], [11], [12] , [13]: The idea of this technique is sending the same query of the mobile users many times; one with his real location and the others with faked locations. The goal of this technique is to confuse the LBS server about the real location of the user. This technique suffers from the problem of the random generation of the dummy locations, where the patterns of the user locations received by the LBS server can be analyzed to infer his real location.

Geographic data transformation [14], [15], [16], [17]: This technique is based on a different concept, where the user represents a locations data owner, and he would like to share this location data with others. The LBS server is then used to host the data of the user. So, to provide the location privacy, a transformation process is applied for the user data using a secret transformation key. After applying transformation process, the transformed data is sent to the LBS server to be hosted and available for sharing. For querying this data, the user who has the secret transformation key can get the locations data back. For this technique, analyzing the access patterns of the LBS services can lead to infer the user transformed locations data, because the same query returns the same encoded location [27].

Private Information Retrieval (PIR) [18], [19], [20], [21], [22], [23]: This technique is based on using cryptography systems to provide the location privacy. In this technique, the user is allowed to access a record from the database of the LBS server, and at the same time the LBS server cannot detect which record is accessed by the user. The privacy of the user's location is achieved by building special hardware for this purpose and embedding the secret keys to the hardware by the manufacturer. This technique has its drawback which is represented by its vulnerability to the misbehavior of the hardware manufacturer.

Location privacy technique based on Paillier public-key cryptosystem [24]: This technique is one of the PIR-based location privacy techniques. This technique provides the location privacy by utilizing the homomorphic properties of the Paillier public-key cryptosystem [25]. Paillier cryptosystem is one of the public-key schemes which can be used to encrypt and decrypt messages using a pair of keys (public key and secret key) for each user. The public key of the user is made available and public for others, while the secret key is kept confidential by the user. In the encryption process, the shared public key of the receiver is used by the sender to encrypt the message, and then the encrypted message is sent to the receiver. In the decryption process, the original message can be retrieved only by the receiver who has the secret key by decrypting the encrypted message using that secret key. In contrast to the other public-key cryptosystems, Paillier cryptosystem has two special homomorphic properties which are utilized by [24] to provide location privacy. The homomorphic properties of Paillier cryptosystem are:

$$\text{Property 1: } E(m_1)E(m_2) = E(m_1 + m_2)$$
$$\text{Property 2: } E(m_1)^{m_2} = E(m_1 m_2)$$

According to the first homomorphic property, multiplying the encrypted values of two messages equals the value of adding the two plaintext messages values and then applying the encryption to the result of the addition. The second homomorphic property shows that raising the encrypted value of the first message up to the value of the second message equals the value of multiplying the two plaintext messages and then encrypting the value of that production.

In this technique, the LBS model consists of the mobile user, the GPS satellites, the mobile network base station and the LBS provider. The mobile user determines his location by receiving and analyzing the signals of the GPS satellites, and then sends his location-based query to the LBS provider using the mobile network. The LBS provider responds to the mobile user query, calculates the query result, and then sends the result via the mobile network to the mobile user. The base station of the mobile network represents the bridge between the mobile user and the LBS provider. There is an assumption that the communication between the mobile user and the LBS server goes through one of the available anonymous services to protect the LBS provider from inferring the location of the mobile user by analyzing the network identifier of the mobile user. The technique divides the working area into a grid of equal-size cells. The model of the technique focuses on supporting the kNN queries which consists of three stages:

1) Query Generation

2) Response Generation

3) Response Retrieval

In the query generation stage, the mobile user generates the query by specifying the cloaking region and encrypting the columns flags. The clocking region is constructed as n□ n cells, while the columns flags represent indicators to the existence of the user in the columns of the cloaking region. So, for each column in the cloaking region, the value of the column flag is 1 if the user is allocated in that column. But if the user is not allocated in that column, then the value of the column flag is zero. After that, the columns flags are encrypted using the Paillier public-key cryptosystem where the public key of the mobile user is used. In the response generation stage, the LBS server generates the response based on the cloaking region and the encrypted columns flags sent by the mobile user. Since the columns flags are encrypted using the public key of the mobile user, the LBS server can't decrypt them and then it is not possible by the LBS server to know which column or cell the mobile user is allocated in the cloaking region.

To generate the response, the LBS server raises each encrypted column flag of every cell in that column in the cloaking region to the data value of that cell which represents the kNN vector of the center of that cell. So, the LBS server uses the encrypted column flags to calculate the response, where this response is also encrypted and the mobile user is the only one who can decrypt it. Based on the first homomorphic property of Paillier cryptosystem, raising the encrypted values of the columns flags to the values of the kNN vectors of the centers of the cloaking region cells has the same value of multiplying the values of the columns flags by the values of the kNN vectors of the centers of the cloaking region cells. Hence the columns flag value is 1 for only the column where the user is allocated in the cloaking region, where the column flag value is zero for the other columns, and multiplying the columns flags with the values of the kNN vectors of the centers of the cloaking region cells gets zeros for all the cells in the cloaking region except the column where the mobile user is allocated. After that, the LBS server multiplies the result of previous step of each cell in the same row to get one value representing each row. Based on the second homomorphic property of Paillier cryptosystem, multiplying the encrypted values has the same value of adding the original plaintext values which all of them represent zeros except the value which refer to the cell of the column where the mobile user is allocated. Once the response is generated by the LBS server, it is sent to the mobile user.

In the response retrieval stage, the mobile user decrypts the values received from the LBS server to get the query result using the secret key of the mobile user. So, by decrypting the value which represents the row where the mobile user is allocated, the kNN vector of the center of the mobile user is retrieved. According to this technique, the mobile user can get the kNN vector of his current cell in the cloaking region without revealing his accurate location to the LBS server, which means providing the location privacy.

Although the technique provides the location privacy for the mobile user, the accuracy of the query result is affected. Calculating the kNN vector of the center of each cell and then using that kNN vector for all the points located inside that cell affects the accuracy of the kNN query. To improve the accuracy, the kNN vectors of the neighbor cells of the current cell of the mobile user are required to improve the accuracy of the mobile user query. So, based on the location of the mobile user inside the current cell, the number of the required neighbor cells to be queries is specified. If the mobile user is allocated in the border of the cell, then the kNN vector of one or three additional cells are needed. As shown in Fig. 2, if the mobile user is allocated in one of the corner sub-cells of the border, then three additional cells are required to be queried. But if the mobile user is allocated in one of the non-corner sub-cells of the border, then one additional cell only is required to be queried.

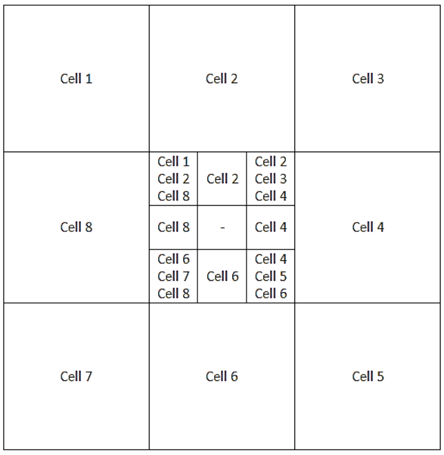

Fig. 2: Number of additional neighbor cells to be queries based on the location of the user

III. PROPOSED SOLUTION

In this paper, the aim is to improve the location privacy technique based on Paillier public-key cryptosystem. As explained in Section II, the reduction of the query accuracy is a result of using the kNN vector of the center of each cell in the working area to be the answer of all the kNN queries allocated in that cell. To reduce that effect, the improvement of the accuracy of the kNN queries is done by querying one or three more kNN vectors of the neighbor cells which increases the communication cost.

So, our contribution is based on:

- Reducing the communication cost by reducing the number of the additional queries which result from querying the additional neighbor cells.
- Improving the accuracy of the kNN queries for the working area which is divided into cells with large size by querying the four sub-cell centers of the current cell of the mobile user instead of querying the neighbor cells of the current cell.

In our first contribution point, the idea of reducing the communication cost comes from our assumption that it is not necessary that all the mobile users who are allocated in the border of their current cell need to query more neighbor cells. According to the original technique in [24], the aim of these additional queries is to improve the kNN query accuracy.

So, our idea is to reduce the communication cost by limiting the process of querying additional neighbor cells for only the mobile users who are allocated in cells with low query result accuracy. To calculate the kNN query accuracy for each cell, the kNN vector of the four corners of each cell is calculated. Then, the similarities between the kNN vector of the center of the cell and the kNN vectors of the corners are calculated. The minimum of the similarities values is considered as the minimum accuracy of the kNN vector of the cell center for that cell. In other words, kNN vector of the cell center can be provided for any mobile user allocated inside the cell with the provided minimum accuracy value which equals to the minimum value of the similarities between the kNN vector of the cell center and the four kNN vectors of the cell corners. So, based on a specific threshold, if the mobile user receives the kNN vector of the center of his current cell, and the minimum accuracy of that kNN vector is smaller than the required level of the accuracy, then the mobile user needs to query the neighbor cells as explained in the original paper. But, if the minimum accuracy of that kNN vector of the center of his current cell is greater than or equals the required level of the accuracy, then there is no need to query the neighbor cells. Based on this, the communication cost is expected to be reduced from 2 or 4 queries –depends on the location of the mobile user in his current cell - to only one query.

In the second contribution point, we are concern on the accuracy of the kNN queries on the cells which have high density of the points of interests (POIs). This situation happens when the working area is divided into cells with large size, and hence each cell has a large number of POIs. In such situation, the important question is: if we want to improve the accuracy of a kNN query which is allocated in the border of his current cell, is it correct to query the cell centers of his neighbor cells? If the current cell of the mobile object has a high density of POIs, then our assumption is ‘Looking inside’ is expected to better than ‘Looking outside’. So, based on this assumption, our second contribution depends on modifying the technique in the original paper, such that for the working area with cells of large density of POIs, then improving the accuracy can be achieved by getting additional kNN vectors by looking inside the cell of the mobile user instead of looking outside it. This can be done by calculating the kNN vectors of the centers of the four sub-cells of the current mobile user cell instead of the neighbor cells as illustrated in Fig. 3.

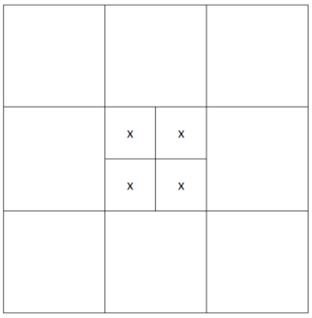

Fig. 3: Querying the current cell sub-centers instead of the neighbor cells

Based on this modification, we expect an increase in the accuracy of the kNN query result, but also an increase in the communication cost for such cells with large density of POIs. The expected increase in the communication cost is due to the use of the four additional kNN vectors of the sub-cells centers instead of using only one or three additional kNN vectors of neighbor cells. So, in order to implement our second contribution point, we need to define a measure to be used in deciding ‘Look inside’ or ‘Look outside’ the cell. So, for a specific threshold value of that density measure, if the value of that measure for the current user’s cell is greater than or equal the threshold, then the centers of neighbor cells of the current user’s cell will be used to improve the kNN query of the user. But if the value of that measure for the cell is smaller than the threshold, then the sub-cells centers of the current user’s cell will be used to improve the kNN query result. The first suggestion was to define the measure as the number of POIs in the cell. But we realized that by using kNN queries with different values of k, we need to involve the value of k in our measure. Therefore, we defined our measure for each cell as the ratio of k to the number of POIs in the user’s current cell. So based on the defined measure, if the value of the measure for the user cell is greater than or equal the threshold, then it means that the ratio of k to the number of POIs of the cell is high, and there is no need to ‘Look inside’ anymore because the kNN vector of the cell center contains a high percentage of the POIs of the cell. But if the value of the measure for the user cell is smaller than the threshold, then it means that the ratio of k to the number of POIs of the cell is low, and there is a need to ‘Look inside’ because the kNN vector of the cell center contains a small percentage of the POIs of the cell and getting kNN vectors of the sub-cells center of the current cell is supposed to improve the accuracy of the kNN query of the user.

Fig.4 shows the flowchart of the technique after the improvement.

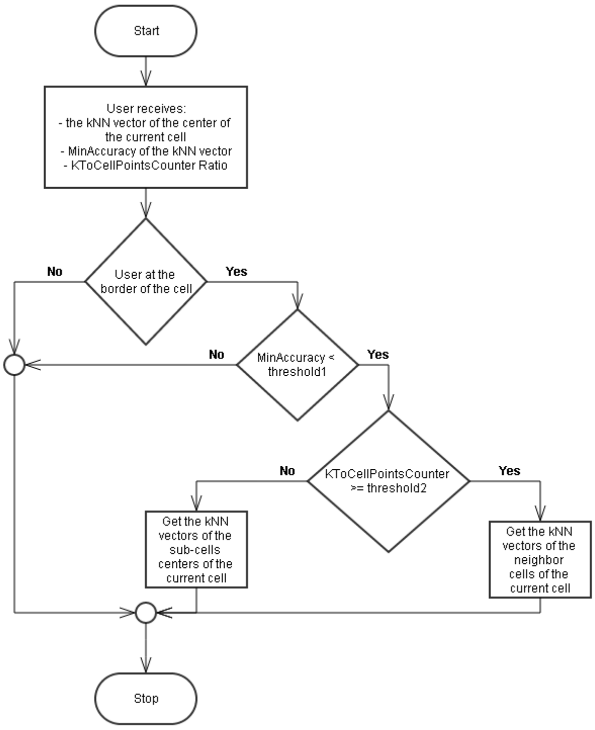
Start
User receives:
- the kNN vector of the center of the current cell
- MinAccuracy of the kNN vector
- KToCellPointsCounter Ratio
User at the border of the cell
No
Yes
MinAccuracy < threshold1
No
Yes
KToCellPointsCounter >= threshold2
No
Yes
Get the kNN vectors of the sub-cells centers of the current cell
Get the kNN vectors of the neighbor cells of the current cell
Stop

Fig. 4: Flowchart of the technique after the improvement

IV. RESULTS (EXPERIMENTS)

To test the performance of our modified technique in comparison to the original technique, we have implemented a prototype which we used it in running the experiments.

To run the experiments, we used the data set [28] which is available on the Internet. The data set contains 123,593 POIs which represent three metropolitan areas which are New York, Philadelphia and Boston. The data set contains also POIs which represent uniformly distributed rural areas and small population centers, which are considered as noise for the clusters of the three metropolitan areas. To run the experiments, 10,000 queries were used which are uniformly distributed on the area represented by the data set. The experiments were run using the different values of the system parameters which are specified in Table 1.

TABLE I. : SYSTEM PARAMETERS

Parameter	Values
Number of Grid Cells (Delta)	50, 100, 200, 300, 400, 500, 1000
K	1, 5, 10, 15, 20
Minimum Accuracy Threshold	0, 0.2, 0.4, 0.6, 0.8, 1
KToCellPointsCounter Threshold	0.2, 0.4, 0.6, 0.8

Fig. 5–10 show the communication cost reduction percentage of our modified technique. As expected, the

communication cost is reduced as a result of using the Minimum Accuracy threshold to limit the number of the additional required queries for neighbor cells. These figures show also that when the delta value increases, the communication cost reduction percentage also increases. Increasing the delta value means dividing the working area into more cells, and then the size of each cell becomes smaller. Based on these figures, it is clear that cells with small size provide kNN vectors with high Minimum Accuracy value for all the mobile users located inside these cells, and then additional queries to improve the accuracy are not required which leads to decrease the communication cost efficiently.

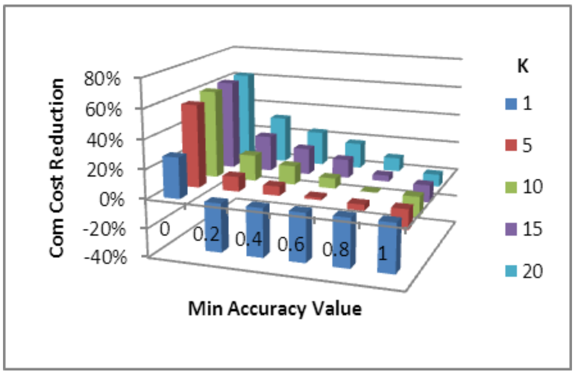

Fig. 5: Communication cost reduction percentage of modified technique (Delta = 100)

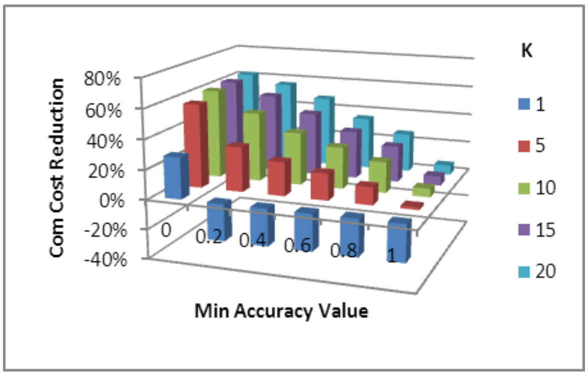

Fig. 6: Communication cost reduction percentage of modified technique (Delta = 200)

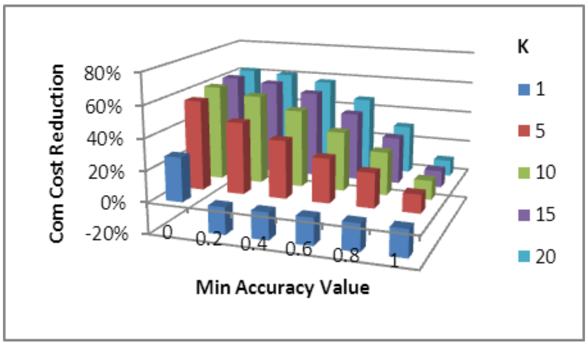

Fig. 7: Communication cost reduction percentage of modified technique (Delta = 300)

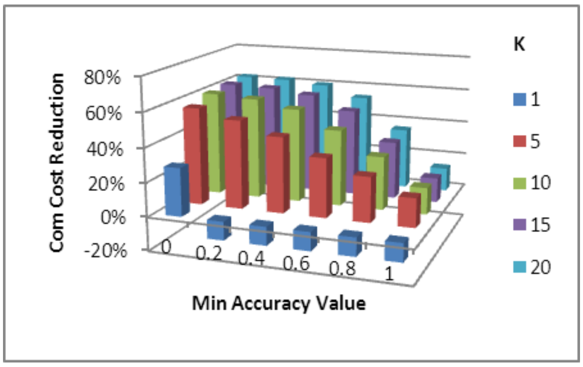

Fig. 8: Communication cost reduction percentage of modified technique (Delta = 400)

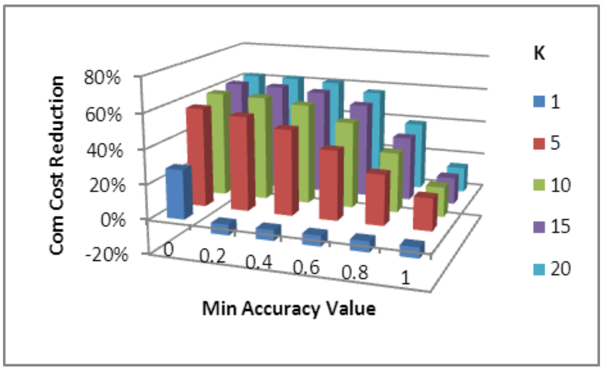

Fig. 9: Communication cost reduction percentage of modified technique (Delta = 500)

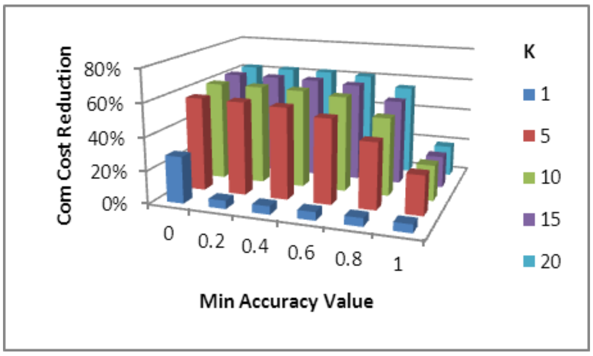

Fig. 10: Communication cost reduction percentage of modified technique (Delta = 1000)

Fig. 11, 12 and 13 show the communication cost average and the accuracy level average of the original technique and our modification for Delta with values 100, 200, 300, 400, 500 and 1000. Fig. 13 shows the communication cost reduction of our modification is 39.4%, where at the same time there is a reduction in the accuracy level of 1.3%. This reduction in accuracy is a result of limiting the number of additional queries required to improve the accuracy which were required by the original technique. So, based on these results, getting a reduction in the accuracy level of 1.3% with reduction in the communication cost of 39.4% represents a good achievement.

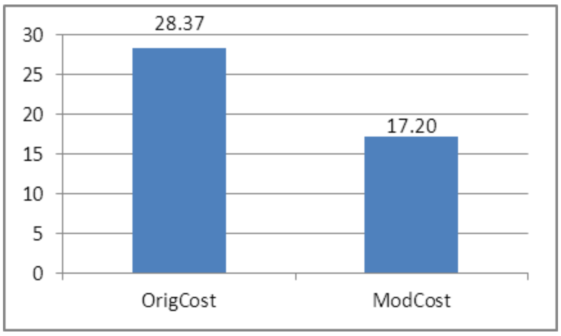

Fig. 11: Average communication cost (Delta = 100, 200, 300, 400, 500, 1000)

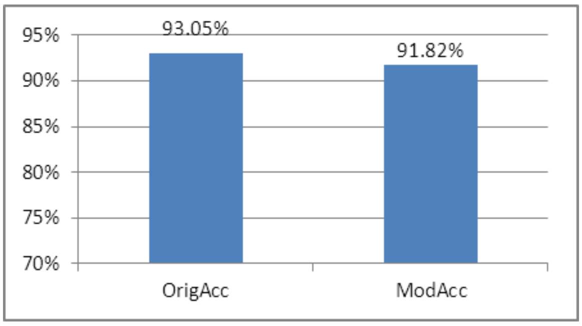

Fig. 12: Average accuracy level (Delta = 100, 200, 300, 400, 500, 1000)

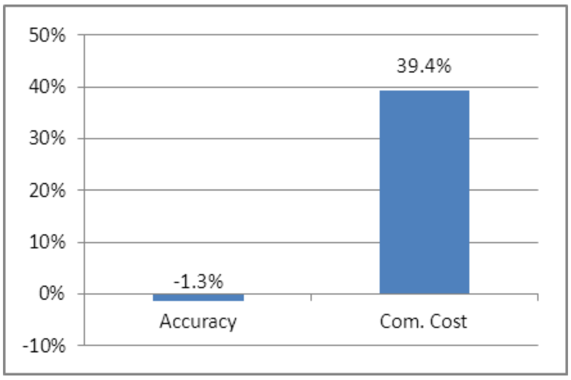

Fig. 13: Modified technique improvement percentage (Delta = 100, 200, 300, 400, 500, 1000)

For our second contribution, fig. 14, 15 and 16 show the result of running the experiments with Delta = 50 and k = 20. These values were used to divide the working area into cells with large size, and measure the effect of improving the accuracy of the kNN queries by using the kNN vectors of the sub-cell centers instead of the kNN vectors of the neighbor cells, where this decision is based on the KToCellPointsCounter measure value of the user's cell. As shown in the figures, the improvement in the accuracy is 5.4% with a 10.3% reduction in the communication cost.

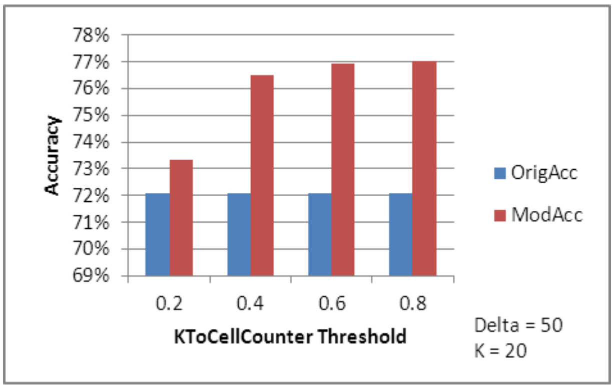

Fig. 14: Accuracy average for the original and modified techniques (Delta = 50, k = 20)

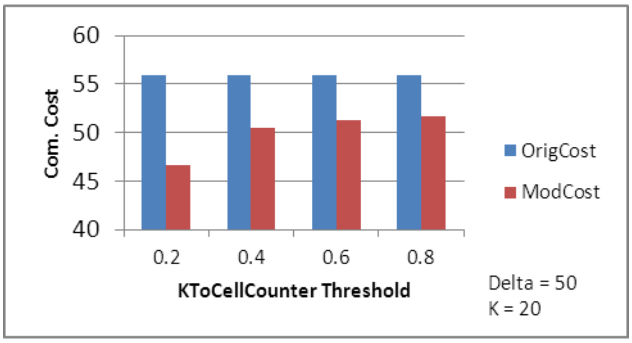

Fig. 15: Communication cost average for the original and modified techniques (Delta = 50, k = 20)

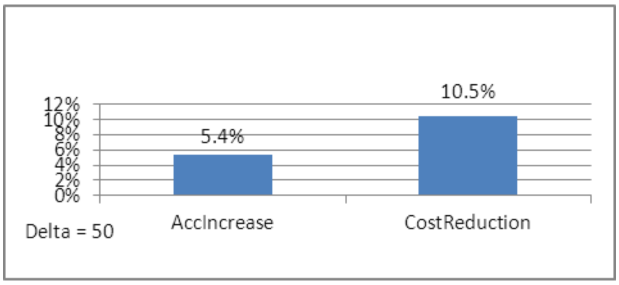

Fig. 16: Modified technique improvement percentage (Delta = 50, k = 20)

V. CONCLUSIONS AND FUTURE WORK

In recent years, Location Based Services (LBSs) market becomes one of the important markets which targets the owners of mobile devices. The importance of the LBSs increases by increasing the dependency of the mobile user on this type of services. Using LBSs introduces the threat of the unauthorized access to the user location data.

Location privacy is an important issue in mobile computing field, where revealing the accurate location of the LBS user leads to infer sensitive information about his life style activities. The objective of this paper was to improve the performance of the location privacy technique using the Paillier public-key cryptosystem by reducing its communication cost. Experiments have shown that our contribution reduces the communication cost up to 39.4 %. Example for practical implementation for this technique is providing location based services with location privacy enabled for mobile objects where the LBS provider is vulnerable to attacks. In the future, we plan to study the performance of the modified technique on different working environments.

REFERENCES

[1] Location-Based Services Market Forecast, Research Report. Pyramid Research. [Online] http://www.pyramidresearch.com/store/Report-Location-Based-Services.htm.

[2] Privacy Protection for Users of Location-Based Services. Kang G. Shin, Xiaoen Ju, Zhigang Chen, Xin Hu. s.l. : IEEE Wireless Communications 2012.

[3] Preserving privacy in environments with location-based applications. G. Myles, A. Friday, and N. Davies. s.l. : IEEE Pervasive Computing 2(1):5664,2003.

[4] Preserving mobile customer privacy: An access control system for moving objects and custom proles. M. Youssef, V. Atluri, and N. R. Adam. s.l. : In Proc. MDM 2005.

[5] Location privacy in pervasive computing. Stajano, A. R. Beresford and F. s.l. : IEEE Pervasive Computing 2(1), 2003.

[6] Supporting anonymous location queries in mobile environments with PrivacyGrid. B. Bamba, L. Liu, P. Pesti, and T. Wang. s.l. : In Proc. WWW 2008.

[7] A peer-to-peer spatial cloaking algorithm for anonymous location-based services. C. Y. Chow, M. F. Mokbel, and X. Liu. s.l. : In Proc. ACM GIS 2006.

[8] The new casper: query processing for location services without compromising privacy. M. F. Mokbel, C.-Y. Chow, and W. G. Aref. s.l. : In Proc. VLDB 2006.

[9] k-anonymity A model for protecting privacy. Sweeney, L. s.l. : Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10: 557 - 570, 2002.

[10] An anonymous communication technique using dummies for location-based services. H. Kido, Y. Yanagisawa, and T. Satoh. s.l. : In Proc. ICPS 2005.

[11] Privately querying location-based services with SybilQuery. P. Shankar, V. Ganapathy and L. Iftode. s.l. : In Proc. Ubicomp 2009.

[12] SpaceTwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile systems. M. L. Yiu, C. Jensen, X. Huang, and H. Lu. s.l. : In Proc. ICDE 2008.

[13] Protecting Location Privacy Based on Historical Users over Road Networks . Qilong Han, Hongbin Zhao, Zhiqiang Ma, Kejia Zhang, and Haiwei Pan. s.l. : In Proc. WASA 2014.

[14] Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism. Haibo Hu, Jianliang Xu, Chushi Ren, and Byron Choi. s.l. : In Proc. ICDE 2011.

[15] Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. Shahabi, A. Khoshgozaran and C. s.l. : In Proc. SSTD 2007.

[16] Secure kNN computation on encrypted databases. W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis. s.l. : In Proc. SIGMOD 2009.

[17] Secure nearest neighbor revisited. B. Yao, F. Li, and X. Xiao. s.l. : In Proc. ICDE 2013.

[18] Private queries in location-based services: Anonymizers are not necessary. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. L. Tan. s.l. : In Proc. ACM SIGMOD 2008.

[19] PRIVE: Anonymous location-based queries in distributed mobile systems. G. Ghinita, P. Kalnis, and S. Skiadopoulos. s.l. : In Proc. WWW 2007.

[20] Nearest neighbor search with strong location privacy. S. Papadopoulos, S. Bakiras, D. Papadias. s.l. : In Proc. VLDB 2010.

[21] Privacy-preserving and content-protecting location based queries. R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. s.l. : In Proc. ICDE 2012.

[22] Privacy-preserving and content-protecting location based queries. R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. s.l. : IEEE Transactions on Knowledge and Data Engineering 2013.

[23] Private information retrieval using trusted hardware. S. Wang, X. Ding, R. H. Deng, and F. Bao. s.l. : In Proc. ESORICS 2006.

[24] Practical k Nearest Neighbor Queries with Location Privacy. Xun Yi, Russell Paulet, Elisa Bertino, and Vijay Varadharajan. s.l. : in Proc ICDE 2014.

[25] Public key cryptosystems based on composite degree residue classes. Paillier, P. s.l. : In Proc. EUROCRYPT 1999.

[26] Protecting location privacy with mix-zones over road networks. Mobimix, B. Palanisamy and L. Liu. s.l. : In Proc. ICDE 2011.

[27] Usable PIR. Sion, P. Williams and R. s.l. : In NDSS, 2008.

[28] [Online] http://www.chorochronos.org/?q=node/60.