AES-Route Server Model for Location based Services in Road Networks

Mohamad Shady Alrahhal
Department of Computer Science
King Abdulaziz University (KAU)
Jeddah, Saudi Arabia

Adnan Abesen
Department of Computer Science
King Abdulaziz University (KAU)
Jeddah, Saudi Arabia

Muhammad Usman Ashraf
Department of Computer Science
King Abdulaziz University (KAU)
Jeddah, Saudi Arabia

Sabah Arif
Department of Computer Science
Superior university Lahore
Lahore, Pakistan

***Abstract*—The now ubiquitous use of location based services (LBS), within the mobile computing domain, has enabled users to receive accurate points of interest (POI) to their geo-tagged queries. While location-based services provide rich content, they are not without risks; specifically, the use of LBS poses many serious challenges with respect to privacy protection. Additionally, the efficiency of spatial query processing, and the accuracy of said results, can be problematic when applied to road networks. Existing approaches provide different online route APIs to deliver the precise POI, but mobile user demand not only Accurate, Efficient and Secure (AES) results, but results that do not threaten their privacy. In this paper, we have addressed these challenges by proposing an AES-Route Server (RS) approach for LBS, which supports common spatial queries, including Range Queries and k-Nearest Neighbor Queries. We can secure the user location through the proposed AES-RS model because it provides the query results accurate and efficiently. The proposed model satisfies the primary goals including accuracy, efficiency and privacy for a location base system.**

***Keywords*—Mobile computing; location based services; location based services (LBS) privacy; LBS accuracy; LBS efficiency; ubiquitous computing**

I. Introduction

Recent years have witnessed the emergence of mobile computing technology as both a ubiquitous and extremely popular paradigm [1], wherein mobile users are capable of accessing information about nearby points-of-interest (POI). The devices used (smart phones, tablets, etc.) are integrated with a global positioning system (GPS), thereby facilitating the usage of location-based services (LBS). In short, location-based services are value-added services that leverage a user's geographic location when making queries. By geo-tagging a query, users are able to receive more personal, and valuable, results. While helpful, this service depends on many factors, including Points-of-Interest, the precise information surrounding the user and their current location, and the inherent need for privacy protection [7].

A basic architecture for location-based services is depicted in Fig. 1, where a mobile user connects to the LBS Server through a communication network. The user then posts a query to the LBS for some location by sending his current location. The LBS then responds to mobile user with the geographically appropriate set of results.

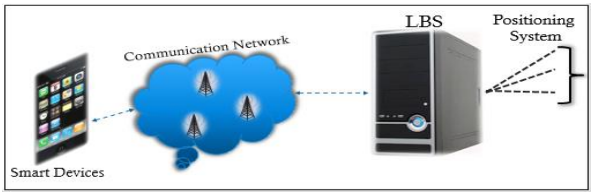


Fig. 1. A common LBS architecture.

In traditional mobile technologies, a mobile user posts a spatial query, q, such as a k Nearest Neighbor (kNN) or Range Query, to a server, requesting particular information; the server will then process the spatial query and return results to the mobile user with appropriate POI information [2], [3]. Without doubt, this "Point-to-Point access model" (POP) is quite ideal and easy to use. Unfortunately, several challenges arise for spatial query processing, such as when there are multiple users and issuing the same query, q, for their POI, or when all mobile users belong to the same location. In these scenarios, the server accrues additional overhead, and resources are wasted [3].

In a conventional mobile computing system, we find three primary goals with respect to a mobile user and the issuance of a spatial query:

- *(G1)* Accurate results,
- *(G2)* Efficient results and
- *(G3)* Privacy protection

G1 and G2 always present challenges due to the inherent realities of a mobile system. Accuracy and efficiency appear as luxuries in a system where both the user and the query are mobile. Additionally, LBS infrastructures and approaches have known limitations with respect to G1 and G2. In terms of G1 for LBS systems, a very famous framework *"SMashQ"* was proposed [5], which supports kNN query processing. The main

purpose of *SMashQ* was to leverage online route APIs, such as Google Maps, Yahoo Maps, Bing Maps, etc. to provide accurate query results for live travel in real road networks. While novel and an advancement in this research domain, SMashQ suffered with efficiency. Each time a user posts a query, q, to any LBS server, the LBS in turn would call the online route API for the most recent results and then return the results back mobile user. In short, the query response times were tragically slow. As expected, the proposed system was very accurate; the overhead of repeated queries on the server, followed by the server repeated calling route API, decreased the entire system efficiency. To overcome this problem, a more efficient approach was proposed, *"Route Server (RS)"* [6]. The primary goal of Route Server was to enhance the system efficiency with respect to query response time by reducing the number of route query requests. Furthermore, they used upper and lower limit calculation approach for this purpose. They also introduced a new mechanism such as *"Query Parallelism"* by parallelizing the query with different scenarios. RS was able to maintain accuracy while avoiding the repeated calls to the server and the online route API. The proposed approach seems to have addressed G1 and G2, leaving only G3.

The rapid growth and ever-increasing number of mobile users brings a variety of new challenges to LBS providers. Privacy protection, G3, is inherently challenging, as users, who want answers to their queries, must, in fact, reveal their locations and potentially sensitive personal data in order to receive answers to said queries.

- What if the mobile user's location is revealed?
- What kind of risks could be faced when mobile user's precise information becomes exposed?
- How can one protect mobile user's location privacy from bad actors?
- What factors should be involved under privacy protection?

These questions have formed the framework for a plethora of research within privacy and security of mobile data systems. A variety of approaches have been proposed to overcome privacy protection related challenges. Many depend on specific scenarios and basic privacy attributes such as the mobile user's identity, his current location, and time information [9]. For instance, a mobile user, who is at an unknown and unimportant location, may have no issue in sharing his personal data. But if the same mobile user is inside a residence or within its proximity, this location data may inadvertently reveal addition information that an adversary could misuse. Accordingly, many privacy attacks were identified, effectively creating a taxonomy of attacks, and respective solutions were proposed, each with its advantages and disadvantages.

A. Location Privacy Attacks

LBS location privacy attacks depend on protection attributes, described previously. Therefore, based on these protection attributes, we have classified Location Privacy Attacks into two major categories as follows (Fig. 2):

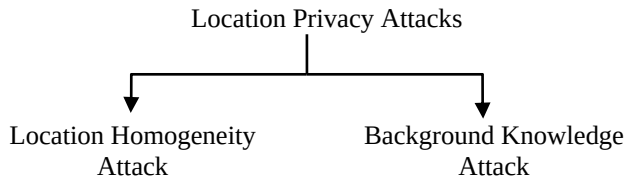


Fig. 2. Classification of location privacy attacks.

1) Location Homogenity Attacks

Location Homogeneity attacks are one the most common attacks seen within LBS systems. They take advantage of the rare case in k-anonymity, where a sensitive value is indistinguishable and posted along a set of k-cluster values. Despite the dataset being k-anonymized, the sensitive value is revealed by any adversary [8], [9]. Additional homogeneity attacks include map utilization by reducing the area. In this case, the adversary reveals the diversity of the position information by analysing some location related information.

2) Background Knowledge Attack

In this attack, the attacker exploits the mobile user's contextual information and is able to accurately predict precise data. The contextual information of the user provides the background knowledge to the malicious attacker. In short, the attacker is able to leverage the background knowledge to prune the set of possible answers.

- **Maximum Movement Boundary Attack** is another background knowledge based attack approach used by adversaries to reveal mobile user's actual information. The adversary discovers the mobile user's region by identifying the maximum movement between two successful POI against posted queries in that specific region [10].
- **Multiple Query Attacks** The attacker follows the query log and identifies the query posted or updated frequently within a specific interval. The attacker effectively shrinks the specific region based on where he got consecutive query updates of a particular k-anonymity set and corresponding actual query [9], [11].
- **Context Linking Attacks** are categorized into three groups: personal context linking attacks, probability distribution attacks, and map matching attacks. Personal context linking attacks are related to the personal contextual information of a mobile user, which might be belong to his preferences or POI. Whereas probability distribution attacks are based on the high probability function of mobile user's location position. An adversary discovers the user's most frequent visited location position, along with a particular time span, and then applies a probability function to identify his precise information. Finally, Map matching is the third context linking attack, wherein a mobile user can be traced for a certain location by removing all irrelevant regions from the Map. Moreover, in order to leak the actual location information, an adversary could use the semantic information gained from the Map [12].

B. Location Privacy Approaches

A variety of approaches have been proposed to solve the aforementioned privacy attacks.

1) K-anonymity

One of the most commonly used approaches for location privacy preserving in LBS system is "K-Anonymity", which insures that the precise information of targeted mobile user is indistinguishable from the value of set K-1 posts to LBS server. We can find out the probability [13] to trace the actual user's data as follows:

Let's have K a set of position of all anonymity users K = {k1, k2, k3, ... ,kn-1}. *Therefore Probability of target user could be discovered as:* $1/K$ (1)

The basic idea of k-anonymity to protect location privacy was demonstrated by Gruteser and Grunwald [31]. The theme of k-anonymity was that a mobile user can post a query, q, to the LBS server with an obfuscation area, along with k-1 anonymity positions of other users, rather than sending his precise location position. Certainty, k-anonymity approach is better in order to achieve the location privacy in LBS system; but in some cases, there are serious challenges when using this approach as follows:

- Homogenous Attack.
- Background Knowledge Attack.

2) Cryptography Based Approaches

Cryptography is another powerful approach to preserve a user's location privacy from malicious attackers in a LBS system. The core idea behind cryptography based approach is utilization of encryption and decryption schemes for precise data that need to be sent over a network. A mobile user posts a query over the network; this query includes his secret data, which is encrypted by apply some particular algorithms at mobile user's end. The same algorithm is available at server side to decrypt the data sent by user and utilized for further processing. The use of encryption and decryption schemes is dependent on the required level and kind of privacy. Cryptography approaches are classified into two main phases and then sub types as shown below in Fig. 3.

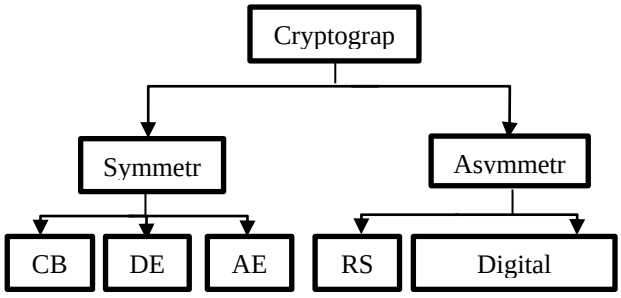


Fig. 3. Cryptography classification.

Certainly cryptography approach is very secured and implementable for LBS system but In contrast, a big challenge for cryptography based approach is the requirement of a massive level of computation during encryption and decryption takes more time than the system required. In LBS system, time is very significant attribute in order to provide the results efficiently. However, implementation of cryptography might be costly regarding to this factor [4].

3) Mix Zones

Beresford introduced a new approach as "Mix Zone" for privacy location protection in mobile computing system [14]. Main theme of Mix zone was to conceal the precise location position of mobile user in his current locating region just like showing that "No existing in this area". Once a mobile user enters in a mix zone area, his ID is shuffled by all other users belonging to that particular zone and the user's precise location is protected. The major challenge for this approach is that an eavesdropper can easily find out the sensitive data of multiple mobile users through limited mix zone area [15].

4) Position Dummies

Leading to privacy location protection in LBS system, a new approach was introduced as "Position Dummies". The fundamental principle of position dummies approach is that, user sends his actual position along with number of dummy location where mobile user' precise information is indistinguishable [16]. Once user change his position from A to B with (x, y) coordinates, he posts a new query by sending his current position along with new dummies according to new place as shown in Fig. 4.

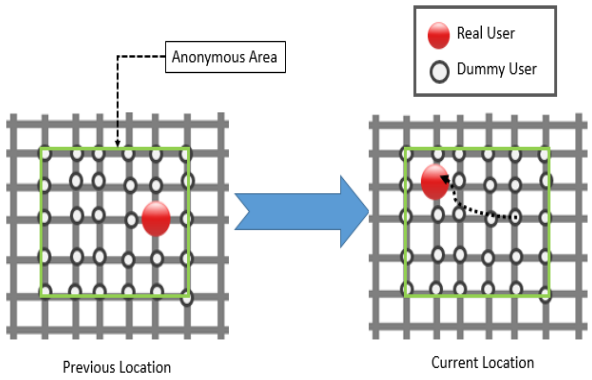


Fig. 4. Dummies on changing position.

In past, it has been remained a major challenge for dummy position that how to generate the number of dummies that have to post along user query to find any route path or POI [17], [26]. Later on, this challenge was overtaken by introducing different tools to generate these dummies [18]. In this paper, we also have proposed an efficient algorithm to generate the dummies at user end and then post to LBS along actual data. Position dummies have been considers the most approachable technique to secure the user's precise location information. In our proposed AES-RS approach, we have implemented "position dummies technique" and made a secured route server approach for location based services in road network as discussed in other section.

The remainder of the paper is organized as follows. Section II describes related work, while the proposed AES-RS approach is discussed in Section III. In Section IV, we have discussed the implementation and results. Finally, Section V discusses the conclusion and future work directions.

II. RELATED WORK

In this section, we have illustrated the existing approaches utilized by others, advantages, limitations and future perspective directions to provide privacy for location protection of these approaches.

W. Sun, C. Chen and B. Zheng [19] emphasized road networks query processing approach. They proposed Network Partition Indexing (NPI) an Air Indexing that was supportive for spatial queries such as Range Query, CNN Query and kNN query. The basic idea of NPI was the processing of these spatial queries on road network by splitting the whole road network into small number of regions. They consider the road network concerning area as a grid G, and make its partition into number of cells where some information like upper and lower limit of each cell, border point and data segment was pre-computed to utilized in future query processing. Once mobile user posted any spatial query for a POI or route path, using these precomputed parameters, server broadcast the results in response through wireless network. They implemented NPI approach in real application and evaluated valued results. The one major challenge using this NPI approach was lost of information in case of link error over the network. They considered error-resilient and efficiency as future related challenges.

Z. Shao, D. Taniar and K. Adhinugraha presented Range-kNN queries supportive approach for privacy protection in [20]. The proposed algorithm was basically consisting of two major parts. In first part, they presented a new approach as Landmark Tree (LT) that was used to discover an appropriate landmark area by concealing the actual user's actual position. For LT, only a radius as parameter was required from mobile user for Range-kNN query implementation. After discovering the query range, another part as search algorithm was implemented to find out the most nearest neighbor from LT. In shortly, first part is responsible to find position inside the query range whereas second part is responsible to discover the location position from outside the range such as *iNN (i > 1).* The proposed algorithm was implementable limited to static objects but not for complex moving objects in real time applications.

B. Niu et al introduced Cashing-Based approach for location privacy protection of user's position in Location Based Service system [21]. Cashing based approach leads basically two algorithms such as CaDSA that was related to k-anonymization to improve privacy through utilizing cashing dummy selections. Leading to CaDSA the author discovers some other performance effecting attributes such as how to normalize distance and how we can make sure the data freshness. Leading to privacy enhancement, the second algorithm called "enhanced CADSA" was proposed. Admittedly, the proposed algorithms provide privacy in location but the overhead of frequent queries to LBS makes the system performance down.

In [22], [23], the authors emphasized on location monitoring challenge for real time distributed system in mobile environment. According to author, the mobile objects should itself be responsive rather than increasing load on central server for objects related computation. In order to develop such a responsive system, they make a set of assumptions such follows:

- The Moving Objects (MOs) have ability to locate its position.
- MOs have ability to determine their velocity vector.
- All MOs existing in mobile environment have ability of computation for assigning tasks.
- There is a synchronized clock among MOs.

They considered that in mobile computing system a distributed approach should be discovered that support *continues moving queries* along moving objects and proposed "MobiEyes". Furthermore, they brought in some optimization approaches constrict self-computation power at MOs end. Admittedly, the proposed approach is valuable but assumptions for such system are still challenges and future work for LBS system.

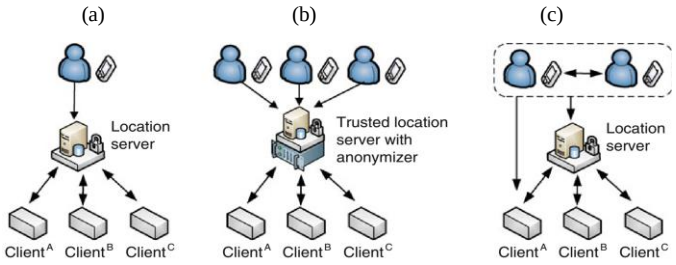
More on privacy protection, as discussed above Route-Server approach is one of the most efficient and accurate query results providing approach in LBS road networks. But the major challenge for RS was privacy protection of mobile user's precise information from adversary who can infer the faulty information in real data when a mobile user wants to post a spatial query for any route path or POI. We grouped privacy goal as G3 in above section.

Leading to G3, Privacy protection is another major challenge for LBS in road networks as it is very common practice to send some personal information when user issues any query for some POI information such as cinemas, bars, friend's location or any route path on a road network. For instance, Let's have a set *Q of queries {q1, q2, q3 … qn}* where each q ∈ Q belongs to Q set and posted as a route query, it will allow to an adversary to infer some false information by revealing mobile user's precise information [4] which is a big challenge for "Route Server" approach. In order to improve the privacy factor in Route Server algorithm we have proposed AES-RS a new secure approach presented in next section.

III. AES-RS SYSTEM MODEL

This section consists of proposed AES-RS system architecture which is essentially enhanced Route Server Architecture. One of the major components of AES-RS model is middleware Location Server that must be considered carefully. However before moving toward AES-RS model, we must introduce briefly the common models of location servers (LS) that are being used in LBS system [27], [28], 30]. These models are assorted into three basic categories including Untrusted Location Server (ULS), Trusted Location Server (TLS) and Peer to Peer based network (P2P) [29] where each model consist of three components as Mobile User Devices, Location Server and clients. In basic scenario each client interact with location server for desired POI or location finding, Location server further contact with clients to get the requested position. From Fig. 5(a) that elaborates the untrusted location server model, Fig. 5(b) shows the trusted location server using anonymizer that ensure trustworthy to deal with dummy position based request model or k-anonymity model

and Fig. 5(c) describes the third option as peer to peer network where each mobile user could interact with other mobile users or devices to find out the desired location or POI [8].



(a) Untrusted Location Server. (b) Trusted Location Server using anonymizer. (c) Peer to peer network.

Fig. 5. Common LBS models.

Subsequently AES-RS is dummy position based model where a request is made along with number of dummy positions, however based on model features, we have selected second option as Trusted Location Server to ensure the provision of locations to mobile devices or users with privacy.

A. AES-RS System Arcitecture

AES-RS (Secured Route Server) architecture is enhancement by location privacy perspectives in Route Server Architecture proposed by [6]. AES-RS system architecture consists of three major entities such as mobile user, LBS and Route API. In AES-RS, mobile user part is now differ as in RS architecture as shown in Fig. 6. We implemented dummy position approach to protect user's location privacy where a mobile user locating to grid area G post a query q along multiple dummies to AES-RS for any route path or *POI*. AES-RS executes that query, find out the required results from local Log *"L"* if find then return the required query results to user otherwise call Route API for the latest results.

In order to approach the goals G3 discussed in previous section, we have modified the definition 2 as "query results" for range and KNN query. Let's a query q a set of dummy positions along actual location locating to Grid G and having time limited T, the results for Range query is:

Q = {k1, k2, k3 ….. kn} then the query resulting definition should be modified q by Q, considering the multiple positions instead of single actual position. However,

$$R = \{p \in \mathcal{P}: \tau t_{now}\ (k \in \mathrm{Q}, \mathrm{p}) \leq T\ )\}$$

And for KNN with K size

$$R = \{k \in Q \in \mathcal{P} : \tau t_{now}\ (k \in \mathrm{Q}, \mathrm{p}) \leq \tau t_{now}\ (\mathrm{k} \in \mathrm{Q}, \mathrm{p}'), \mathrm{p}' \in \mathcal{P} = -R\ \}$$

According to our AES-RS approach, before posting query to LBS, measure the minimum (L lower limit) and maximum (U upper limit) width and height of the specific area called grid "G". The purpose to determine (L, U) coordinates is to make partition of "G" into equal number of cells "Ci". Each cell (E, V) ∈ C representing that cells are connected through set of V Vertices and E Edges where (v ∈ V) and (e ∈ E) as shown in Fig. 7. Further to generate dummy positions, vertices are calculated beyond each cell and one cell position is attached to mobile user's actual position. Finally, an array is generated that contained all dummy K positions and index of actual user's position by following the proposed algorithm DDA (Dummy Data Array.

Algorithm: DDA (Dummy Data Array)

Input: User location (X, Y), Anonymous_Area A, Anonymity_Number K;
Output: array[K(x,y) + (X,Y)]
Procedure:

```
1: G(L, U)      \\ Calculate Both Height and Width, U,L limit.
2: C ← √ G      \\ Calculate Number of cells in G
3: (V,E) ∈ C    \\ Determine vertices and edges of each cell.
4: Px ← Random (0, v(C-1)) , Py= ← Random (0, v(C-1))
5: array[0 to C][ 0 to C]   \\ Initialize 2-D array
6: i = 0, j =0 , x,y=0   \\ Initialize values upto x-axis, y-axis
7: While (i < (C-1))   \\ Fill array with dummy positions
8:              While (j < (C-1))
9:              if ( Ci.posX != X and Cj.posY != Y)
10:                     x ← C.posX , y ← C.posY
11:                     array[i][j] ← x , y
12:                     j ++;     // Repeat step 8
13:             end if
14:             end loop
15:     i ++;                     // Repeat step 7
16:     end loop
17: add Px,Py in array
18: Return array
```

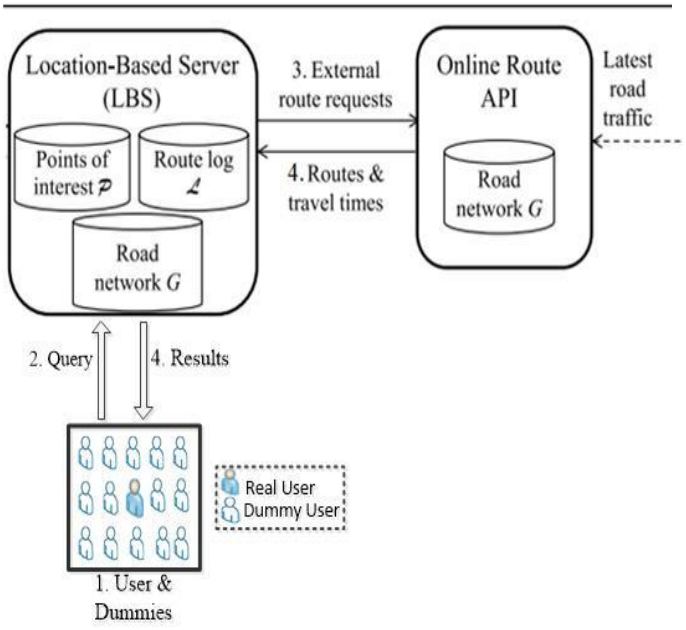


Fig. 6. RES-RS system arcitecture.

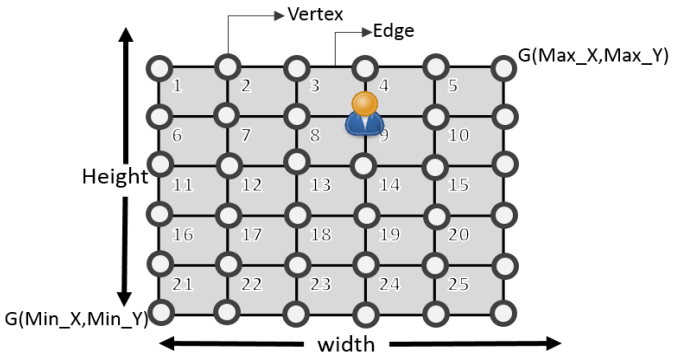


Fig. 7. Grid partition into cells.

According to DDA algorithm, it takes three input parameters as *(X,Y)* coordinates of user locating at current position, anonymous area A which is required to generate anonymity data and K number of dummies which are required to generate. It consider the anonymous area A as grid G and first calculate the upper and lower limits of whole anonymous area with respect to height and width denoted as *<Min_X/ Min_Y, Max_X / Max_Y>*. By using computed LU limits, anonymous area A partitioned into equal number of cells *(Ci ∈ G)* according to given input number of K as in equation 2 that was discovered by equation 3.

$$|C1|C2|C3|C4|- - - - - |Cn| = 1 \quad (2)$$

$$Number\ of\ Cells = \sqrt{G} \quad (3)$$

Once, number of cells are defined, it calculates the vertices and edges beyond each cell mentioned in step 3. Now, assign the mobile user's current location (Px, Py) to one random cell from G. Next, declare an array that will contain all the dummy positions and fill it according to number of cells because each cell is located with one dummy position. Once the array with dummy positions is filled, it adds the index of user's actual position in array and return.

B. AES-RS for Spatial Queries

As AES-RS is supportive for spatial queries such as Range query and KNN query as well. In this section, we present the consequences of Secured Route Server approach for spatial queries for a given query point q, along with a value d and data set P that reduce the number of requests. As described above, for AES-RS approach, we have used a Trusted Location Server (TLS) which ensure that only actual query request posted from mobile device to TLS along with set of dummy locations array will be computed to determine the POI or desired location. However, there will not be any change in spatial queries.

For range query in AES-RS, it first comport the distance range search for data set P on G road graph from q query point, denoted as range (q, d, P) = {o | o ∈ P ∧ ‖ o, q ‖ ≤ d} and then store the retrieved results from range in a set R. Similarly for KNN query with given query point q with data set P on G road network, a K Nearest Neighbor (KNN) query determine the k objects in P whole network distance which is represented as follows:

$$kNN(q,k,p) = \{O = U_{i\in[1,k]}{}^{o_i} | O \subseteq P \wedge \forall\, o \in \acute{P} - O, \forall\ o_i \in O, \|q,\acute{o}\| \geq \|q,o_i\|\}.$$

Unlike range query, KNN query doesn't have the fixed area for searching and contingent upon the current location of query point q and k value it find out the candidate point by defining upper and lower bounds.

C. AES-RS Effects on Accuracy

The one objective of RS algorithm was to provide accurate query results. As accuracy assurance in RS algorithm was achieved by calling route API frequently to get most updated query results and generate log L for Ψt routes that is validate till δ expiry time otherwise expire routes Ψt. In case of dummies along actual position, certainly it requires larger space to manage log L but no effect on accuracy in query results. However we can manage L by adding more memory space in the system.

D. AES-RS Effects on Effecincy

Efficiency was another essence factor in AES-RS and achieved by maintaining Ψt routes log L. Definitely, it will affect on query response time because of requiring number of locations, doesn't matter it is dummy or actual location, LBS processing is required. But powerful approach as log L, POI and Road Network G at LBS maintain route path and minimize the overhead of frequent route API calling.

IV. Experemental and Results

In this section we demonstrated our AES-RS approach and simulated to evaluate performance after enhancing RS approach by privacy factor. We used Riverbed Modeler academic edition 17.5 simulator tools that can be used to drive accuracy and performance in real network applications. Its old name was OPNet Modeler [24]. In our experiments, we used france_highway road network map provided in riverbed modeler. Further we selected multiple nodes as actual user location where he wants a route path to find out the nearest ATM from his current location using over the road network. In order to protect his precise information as current location, we draw multiple dummy positions *(k-1)* then posted a query containing actual location along generated dummy positions to LBS server through a wireless network. The tenure in which multiple queries were posted to LBS and it respond back with query results was evaluated by setting 1 week duration. By following a basic wireless network routing approach, we used two Ethernet routers and sixteen dummy nodes from different locations were connected to each, which is further linked to an Ethernet switch and it post user's query to LBS for query results. Fig. 9 illustrates the rate at which data packets are being received by LBS server sending from Ethernet switch. The delay in transferring data packets to LBS server were calculated by using *"Little's theorem"* [25].

$$N(t) = A(t) + B(t) \text{ and } t \geq 0 \quad (4)$$

Where A (t) is the number of data packets which are arrived at in time (0, t) and B (t) is the number of data packets that are depart from source location in time (0, t).

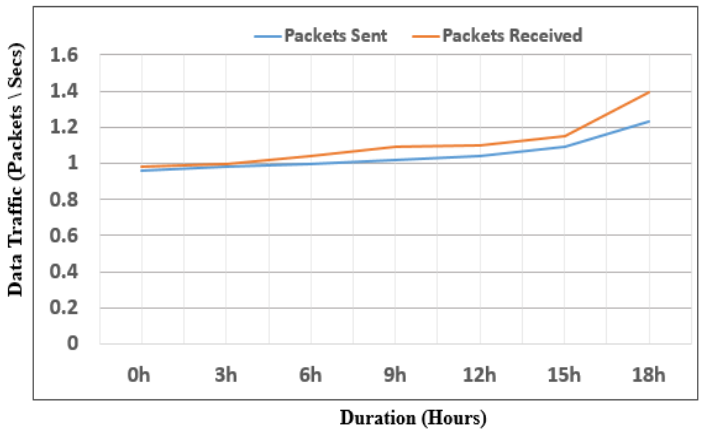


Fig. 8. Data transferring rate to LBS.

We observed that there were some other constituents like data transferring rate as shown in Fig. 8, the delay at Ethernet or wireless communication which could be cause of decreasing AES-RS system performance. In our case as shown in Fig. 9, during query transmitting over the network, delay size is very small in Ethernet and wireless which couldn't be reason to decrease system performance. In Ethernet, it becomes constant at a certain level by assuming that loss ratio in data packet is consistently zero. In contrast, delay variation increase and decrease after a certain time period which was overhead of using LBS as single server. It could be maintained by utilizing multiple LBS servers applying distributed approach.

The most significant part of AES-RS was to maintain LBS performance in order to provide user's query response accurately and efficiently by protecting mobile user's precise location. We evaluated LBS server performance when multiple query requests posted to it for any route path or POI and query processing at server side to return query results. Graph in Fig. 10 shows the number of requests posted to LBS server and its response quick by using log L, POI and Road Network G inside LBS.

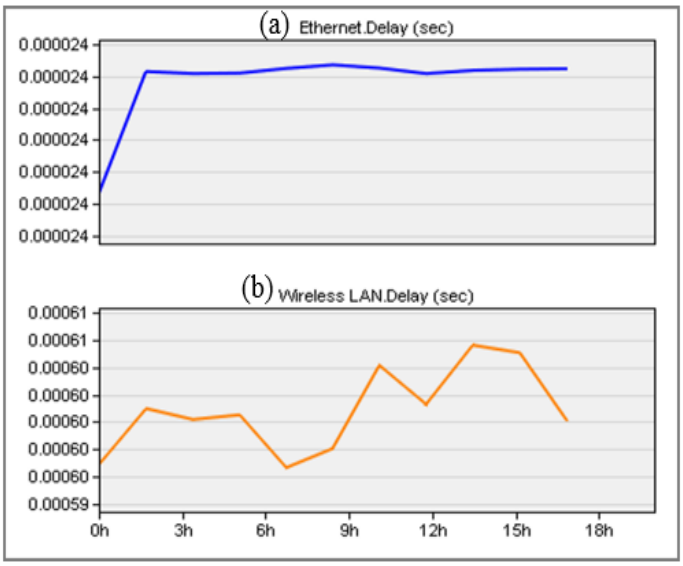


Fig. 9. Delay in ethernet and wireless LAN.

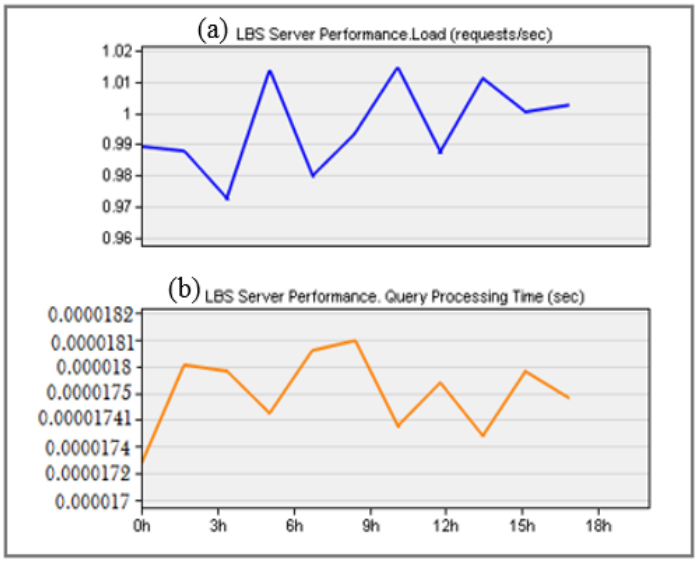


Fig. 10. LBS server performance.

We also evaluated the route API data access rate depicted in Fig. 10(a). The gradually decrease in graph 9 (a),(b) the clearly shows the advantage of log L, POI and Road Network G usage at server side that minimize route API hit rate due to availability of data at LBS server side. At initial stage, due to empty data in log it required to call route API for updated query results that increased route API retransmission attempts rate Fig. 10(b). But after a certain time t, when log L contained number of query results it decrease route API attempt rate. Furthermore, we assessed parallel route path approach proposed in RS algorithm and implemented in our experiments. Fig. 11(a), shows the results of data access delay through route API where we implemented parallel route path approach at LBS server side, it recognize firstly the required path against any mobile query, then it evaluate the relevant queries which are required route Path or POI from the same route. In this way, it minimizes the data access delay along query hits to LBS server.

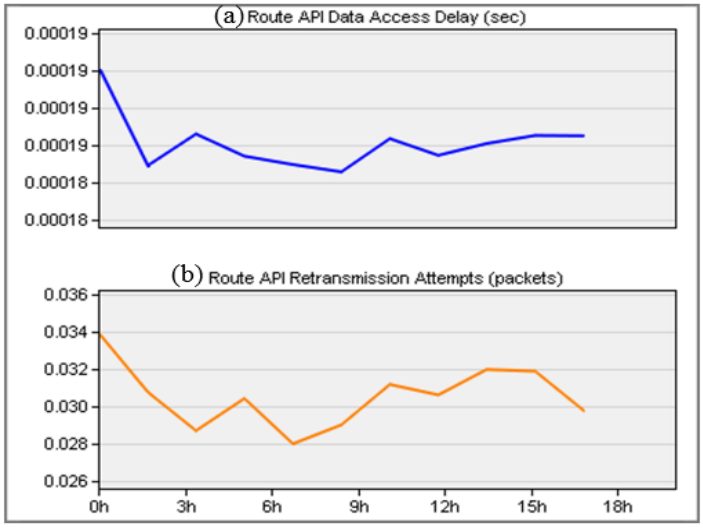


Fig. 11. Route API rerensmission attempts and data access rate.

V. CONCLUSION

In mobile computing environment, every LBS system requires three primary goals such as accuracy, efficiency and privacy. A significant research has been attempted and delivered different LBS approaches to attain these goals. Route Server (RS) is one of the approaches that provide LBS system with accurate and efficient results for spatial queries. But RS algorithm didn't consider G3 as privacy goal to protect mobile user's precise information. However, by location privacy perspectives, we proposed AES-RS architecture which is an enhancement of RS algorithm and protect mobile user's precise location information from any adversary. On behalf of adversary attacks for LBS system, we discussed different kind attacks and various approaches to overcome these attacks. We also highlighted the advantages and limitations in existing approaches. After a critical analysis, we selected dummy position approach that ensure mobile user's privacy protection in RS algorithm and proposed a new approach AES-RS as Secure Route Server Architecture. As generating number of dummies for Dummy Position approach was a major challenge, we proposed an algorithm where dummy positions are generated at user end. Further in term of evaluation (G1, G2, G3) goals we simulated our approach using Riverbed modeler and generated different results. We discussed Ethernet and wireless WLAN as the factors that could be effective in efficiency in LBS wireless network system. From experiment results evaluation we can say AES-RS is an appropriate approach for LBS system which secure the user privacy for location protection by providing accurate and efficiently query results. By future perspectives, it required to examine the proposed solutions at large scale.

REFERENCES

[1] G.H. Forman, and J. Zahorjan. "The challenges of mobile computing."Computer 27.4 (1994): 38-47.

[2] W. Sun, et al. "An Air Index for Spatial Query Processing in Road Networks." Knowledge and Data Engineering, IEEE Transactions on 27.2 (2015): 382-395

[3] M. Wernke, et al. "A classification of location privacy attacks and approaches." Personal and Ubiquitous Computing 18.1 (2014): 163-175

[4] D. Zhang, C.-Y. Chow, Q. Li, X. Zhang, and Y. Xu, "SMashQ: Spatial mashup framework for k-NN queries in time-dependent road networks,"Distrib. Parallel Databases, vol. 31, pp. 259–287, 2012.

[5] L. Yu, and M.Y. Lung. "Route-Saver: Leveraging Route APIs for Accurate and Efficient Query Processing at Location-Based Services." Knowledge and Data Engineering, IEEE Transactions on 27.1 (2015): 235-249.

[6] A. Civilis, C.S. Jensen, and S. Pakalnis. "Techniques for efficient road-network-based tracking of moving objects."Knowledge and Data Engineering, IEEE Transactions on 17.5 (2005): 698-712.

[7] G.K. Shin, et al. "Privacy protection for users of location-based services."Wireless Communications, IEEE 19.1 (2012): 30-39.

[8] W. Marius, et al. "A classification of location privacy attacks and approaches." Personal and Ubiquitous Computing 18.1 (2014): 163-175.

[9] G. Ghinita, M.L. Damiani, C. Silvestri and E. Bertino. "Preventing velocity-based linkage attacks in location-aware applications" In: Proceedings of the 17th ACM SIGSPATIAL international conference on advances in geographic information systems (GIS '09), Seattle, Washington, pp 246–255, 2009.

[10] M. Gruteser and D. Grunwald "Anonymous usage of location based services through spatial and temporal cloaking". In: Proceedings of the 1st international conference on mobile systems, applications and services (MobiSys '03), San Francisco, California, pp 31–42, 2009.

[11] J. Krumm. "Inference attacks on location tracks", In: Proceedings of the 5th international conference on pervasive computing (Pervasive '07). Springer, Toronto, pp 127–143, 2007.

[12] G.Z. Ignatov, K.K. Vladimir, and R.S. Krachunov. "An improved finite-time ruin probability formula and its Mathematica implementation." Insurance: Mathematics and Economics 29.3 (2001): 375-386.

[13] G. Singh, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." International Journal of Computer Applications 67.19 (2013): 33-38.

[14] A.R. Beresford, F. Stajano. "Mix zones: user privacy in location-aware services". In: Proceedings of the second IEEE annual conference on pervasive computing and communications workshops (PerCom '04 Workshops), pp 127–131, (2004).

[15] M.L Yiu, C.S Jensen, J. Møller and H. Lu "Design and analysis of a ranking approach to private location-based services". ACM Trans Database Syst 36(2):1–42, (2011).

[16] K.G. Shin, et al. "Privacy protection for users of location-based services." Wireless Communications, IEEE 19.1 (2012): 30-39.

[17] J. Krumm. "A survey of computational location privacy." Personal and Ubiquitous Computing 13.6 (2009): 391-399.

[18] W. Sun, et al. "An Air Index for Spatial Query Processing in Road Networks." Knowledge and Data Engineering, IEEE Transactions on 27.2 (2015): 382-395.

[19] Z. Shao, D. Taniar, and K.A. Maulana. "Range-kNN queries with privacy protection in a mobile environment." Pervasive and Mobile Computing (2015).

[20] B. Niu, et al. "Enhancing privacy through caching in location-based services." Proc. of IEEE INFOCOM. 2015.

[21] B. Gedik and L. Liu. "Mobieyes: Distributed processing of continuously moving queries on moving objects in mobile system."Advances in Database Technology-EDBT 2004.Springer Berlin Heidelberg, 2004. 67-87.

[22] K. Jürgen. Continuous queries over data streams-semantics and implementation. Diss. Universitätsbibliothek Marburg, 2007.

[23] V. Sercan, and E. ERDEM. "Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard." International Journal of Computer Networks and Applications (IJCNA) 2.3 (2015).

[24] Little, D.C. John, and C.G. Stephen. "Little's law." Building Intuition. Springer US, 2008. 81-100.

[25] L. Hua, C.S. Jensen, and M.L. Yiu. "Pad: privacy-area aware, dummy-based location privacy in mobile services." Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access. ACM, 2008.

[26] A. Monika, and P. Mishra. "A comparative survey on symmetric key encryption techniques." International Journal on Computer Science and Engineering 4.5 (2012): 877.

[27] T. Jawahar, and N. Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis."International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.

[28] P. Gilbert, L.P. Cox, J.W Jung. "Toward trustworthy mobile sensing". In: Proceedings of the 11th workshop on mobile computing systems and applications (HotMobile '10), Annapolis, Maryland, (2010) pp 31–36.

[29] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun and A. Williams "A data privacy taxonomy", Proceedings of the 26th British national conference on databases: the final frontier (BNCOD 26), Birmingham, UK, (2009) pp 42–54.

[30] M. Gruteser and D. Grunwald, Anonymous usage of locationbased services through spatial and temporal cloaking, in ACM MobiSys'03: Procedings of the 1st international conference on Mobile systems, applications and services, pp. 31–42, 2003.

[31] A.R Beresford, and F. Stajano. "Mix zones: User privacy in location-aware services." Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004.