Computer and Information Science; Vol. 8, No. 4; 2015
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Trusted Base Stations-Based Privacy Preserving Technique in Location-Based Services

Muhammad Aqib[1] & Jonathan Cazalas[1]

[1] Department of Computer Science, College of Computing and Information Technology, King Abdulaziz University, Saudi Arabia

Correspondence: Jonathan Cazalas, Department of Computer Science, College of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. E-mail: mpervez@stu.kau.edu.sa/jcazalas@kau.edu.sa

Received: October 23, 2015 Accepted: November 3 2015 Online Published: November 6, 2015

doi:10.5539/cis.v8n4p93 URL: http://dx.doi.org/10.5539/cis.v8n4p93

Abstract

With the advent in mobile and internet technologies, there is a significant increase in the number of users using smartphones and other internet based applications. There are a large number of applications available online that use the internet and provide useful information to the users. These include ones that provide location-based services e.g. google maps etc. These applications provide many facilities to the users who want information regarding a specific area or directions using an optimal path to a destination. Due to these reasons, the number of clients using these applications is increasing on a daily basis. Although these services are very useful and are making it easy for us to get information about our surroundings, some issues are also linked with the use of these applications and their services. One of the more significant issues of using these services is privacy with respect to sending personal location information to location-based services servers. Researchers have provided many solutions to solve these issues. One of the solutions is through caching and use of k-anonymity techniques. In this paper, we have proposed a method to solve the privacy issue that uses caching data approach to reduce the number of queries sent to the location-based services server. We also discuss the use of the concept of k-anonymity when no relevant data is available in cache, and queries are sent to the server.

Keywords: caching, k-anonymity, location-based services, privacy

1. Introduction

Rapid growth in the number of mobile users, and the availability of smooth and stable wireless network facilities, have introduced many applications that could be used to perform many useful operations using mobile devices. Due to these reasons, there is an influx in the number of users using location-based services. Users can download software applications available for free, or by paying nominal prices, and can avail the services provided by different vendors. Today, the main source of these applications are Apple and Google. Google Play Store provides downloadable applications that are android compatible while Apple Store provides applications for all kinds of Apple-devices. There are many applications that may help users to query their locations ex. Google Maps etc. Some applications give the optimized path between the home and the workplace. They also provide information regarding the traffic loads on certain roads at specific times, hence providing the users the facility to choose the best suitable route during rush hours. By using these applications, users can get information about their location and route information. They may also query about the nearby restaurants, hospitals, gas stations, schools etc., by sending queries to the location-based servers. These location-based services are provided to the users by using their location information.

Whenever a user sends a query to a location-based server, he need to send his location information to the server so that the required information within that region could be returned to his device. This may pose a security risk for the user as there may be an adversary who may get location information of the user during the transfer of information. This can allow for the user to be tracked and can lead to misuse of his personal information as well as location. As such, it can be stated that, although these services are widely used, they may cause serious privacy issues for the users (M. F. Mokbel, 2007). Therefore, there needs to be a mechanism to protect the user's privacy when he is going to contact the location-based server. In order to provide privacy and security to a user when he is communicating with the location-based server, many privacy protection schemes have been proposed

by researchers (B. Niu, Q. Li, X. Zhu, G. Cao and H. Li., 2014) (Puttaswamy et al., 2014) (Shin, K. G., X. Ju, Z. Chen and X. Hu., 2012). Also, many approaches have been proposed by researchers to be used as a mechanism while addressing the privacy and security issues in location-based services. Some of the most commonly used approaches are: k-Anonymity, obfuscation, and cryptography-based approaches.

k-anonymity is a general privacy concept used in location-based services. For location-based services, Gruteser and Grunwald used this approach and proposed a solution for location-based services. (Gruteser, M., & Grunwald, D., 2003). The main idea behind the approach used by them was that the user sends his location information and the position of other k-1 users (dummy) to hide his location from the location-based server. The server in return will return the required information but it is hard for it to identify the actual user among the k users because all the users (actual user and dummy users) belong to the same region in range. This was the basic idea behind the k-anonymity concept. Later, researchers worked on it and made some changes to it. In (Zhang, C., & Huang, Y., 2009), authors have used the same concept with some additions to it. They have introduced the idea of strong k-anonymity by adding the factor of reciprocity to the k dummy users. Bamba et al. in (Bamba, B., Liu, L., Pesti, P., & Wang, T., 2008) proposed another variation of this idea by introducing the idea of l-diversity. He achieved the anonymity by hiding the user's actual location in many other diverse locations in the region. For this purpose he sent information about nearest clubs, rail stations, malls, churches, etc. These places were not only different from others, but also not close enough. According to authors, utilizing this method makes it is more difficult for the intruder to find the actual user when they are located far from each other. Adding to l-diversity approach, Li et al. in (Li, N., Li, T., & Venkatasubramanian, S., 2007) have introduced a parameter to calculate the distance between all the actual and dummy locations and a threshold is defined so that the distance between them should be less than its value.

The concept of location Obfuscation is also used in privacy-based approaches. This approach reduces the probability of sending the exact information about user's location and hence improves privacy. Ardagna et al. (Ardagna, C. A., Cremonini, M., Damiani, E., Di Vimercati, S. D. C., & Samarati, P., 2007) proposed a method using obfuscation where a user is supposed to send a circular region to the location-based server while querying instead of sending the exact location. In this way, they do not need to send any kind of additional information like dummies. The drawback of this approach is that when a user is not sending his exact location, he may not get useful information from the server and hence the quality of the data is compromised. Later, R. Chent et al. in (Cheng, R., Zhang, Y., Bertino, E., & Prabhakar, S., 2006), improved this idea by suggesting the use of obfuscation graphs instead of using simple figures like circle mentioned above. In (Yiu, M. L., Jensen, C. S., Møller, J., & Lu, H., 2011), Yiu et al. have presented a framework, "SpaceTwist". In their proposed framework, they have introduced the idea of anchor entity to communicate to the server by sending queries from different locations. Once it receives the data information from the server, the actual user calculates the exact results by using the distance and other differences from the anchor entity.

Cryptographic techniques are also used for the secure communication between the users and the location-based server. But, it seems that these approaches are limited to the communication between the users and their friends within the same region through the use of location-based services. In (Mascetti, S., Freni, D., Bettini, C., Wang, X. S., & Jajodia, S., 2011), authors have proposed a method that uses this approach to notify the friends of a user when they lie in the same area but does not reveal their location information to the location-based server. Private information retrieval (PIR) is also used to enhance privacy. Using this approach, a location-based server is supposed to answer the user queries but it has no information about the user's location due to encrypted data communication between the nodes that only know the way to decrypt the message. Another approach proposed by Marias et al. (Marias, G. F., Delakouridis, C., Kazatzopoulos, L., & Georgiadis, P., 2005) has introduced the idea of distributed sharing of user's location information on different servers for privacy. To retrieve the exact information, the user need to recollect all the shares distributed on different servers. In this scenario, if there is an adversary monitoring the user's data in some location-based server, he cannot get the correct information because he does not have the complete information about the user. However, the problem with this approach and other cryptographic approaches is that it is hard to get some information from the location-based server. This results from the lack of useful input being sent to the server.

In order to provide a secure channel to the users sending queries and receiving data from the location-based servers, B. Niu et al. (Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H., 2015) have proposed a caching based mechanism to enhance privacy while contacting the location-based servers. According to them, it is not safe for the users to send queries to the location-based servers repeatedly. Instead, the information returned from the server in return to the user queries may be cached to be used in future. So before sending queries to an untrusted server, a user first needs to check the data stored in cache. If the data relevant to the user's query is available in

cache, it will be returned to the user. Otherwise, his query will be forwarded to the location-based server. However, the issue at this point is how to protect the user privacy while sending his location and other information to the location-based server. To ensure user's privacy at this stage, authors have used the k-anonymity technique in their proposed method in addition to caching.

The solution provided by the authors could be divided in two parts, caching and querying with k-anonymity. To, cache data, they have used Wireless LAN Access Points (APs). For communication with the untrusted location-based servers, they have proposed two algorithms to select dummies for the purpose of k-anonymity. The algorithm are "caching aware dummy selection algorithm (CaDSA)" and "enhanced caching aware dummy selection algorithm (enhanced-CaDSA)". CaDSA provides a mechanism to randomly select dummies from a list of dummies with same query probability. For this purpose, they first short list the dummies in different classes based upon their query probability. In enhanced-CaDSA, they have added two more attributes to improve the effectiveness of the algorithm. First, they provided the mechanism to check the freshness of data cached in APs. Second, they calculated the normalized distance between the actual user and the dummies to make sure that the dummies are selected from the same region. This way the dummy selection process is more accurate and when the query is sent to the location-based server, data that is more relevant is collected and thus stored in cache. This also improves the cache-hit ratio for future queries.

In this article, we have worked on the above mentioned method to improve privacy. We also have used the idea of caching to store the information returned by the location-based server for future use. However, in contrast to the authors, we have used the distributed approach and have used the idea of base-stations (Gedik, B., & Liu, L., 2004) to cache data so that it could be available to a large number of user. In case of APs used by the authors, the availability of the cache data is very limited because of the small coverage area of APs. Users that fall within the coverage area of a base-station send queries to that base-station and result is returned to them whether from the cached data or from the location-based server. As such, they do not suffer from the problem of finding no coverage area when moving in a car or on roads. This makes this approach more realistic.

We also have provided an improved mechanism to select dummies for the purpose of k-anonymity. Instead of selecting dummies from surroundings, say falling within the circle, we have used the concept of user trajectory. This is a more convenient solution because it collects dummies that are relevant to him and ignores the others. Further, to narrow down the selection area, we have used the concept of view field (Yi, S., Ryu, H., Son, J., & Chung, Y. D., 2014). For this purpose, we define a sector size based on the spatial information and the dummies that fall within that sector are considered. From those dummies, we select ones with the same query probability as the actual user and then at random the required number of dummies are selected. This increases the cache hit ratio and in return reduces the number of queries sent to the location-based server and improves privacy.

In general our contributions are as follows:

- Use of base-stations to cache data increases its capacity and makes it available whether you are a pedestrian or moving in a car.
- Retrieval of user's trajectory information for selection of dummies.
- Defining sector along user trajectory to select only those dummies that fall within his area of interest.
- Proposed algorithm, that selects dummies based upon their query probability and other selection conditions as mentioned above.

The remainder of the paper is organized as follows. Section 2 gives an overview of the work done by other researchers in the field of privacy. Our proposed solution has been discussed briefly in Section 3. The results have been presented in Section 4 and finally we have concluded the discussion in Section 5.

2. Related Work

Privacy in location-based services is a popular and important topic. Many approaches have been proposed by different researchers that deal with different issues with the security of users availing the location-based services (Zhu, Z., & Cao, G., 2011) (Shin et al., 2012) (Li, Q., & Cao, G., 2013) . Although solutions based on the cryptographic (Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J. P., & Aad, I., 2011) and other policy-based techniques have also been used by some researchers, these are not very popular due to the issues related to these types of techniques. Most of the researches are based upon the concept of anonymity, location obfuscation etc. In these kind of techniques, queries are sent to the location based servers to retrieve spatial information and as they directly send their information to a server, the factor of anonymization or the obfuscation is added, as described earlier in this paper. These kind of approaches work fine in order to get related information from the server, but they also face some problems, like single point of failure and bottleneck issues etc. Also if an intruder gets

control of that server, he can easily get the information stored in it and hence create a serious security risk for the users.

Privacy approaches proposed for applications running on mobile devices normally try to avoid these kind of problems. For this reason, many other solutions like VHC mapping (Pingley, A., Yu, W., Zhang, N., Fu, X., & Zhao, W., 2009), method to use cloaking box with k-anonymity (Hu, H., & Xu, J., 2009) and other similar solutions (Pingley et al., 2011), target the computational and storage capabilities of the mobile devices and proposes the solution to minimize the use of their resources. As mentioned above, some researchers have used the idea of k-anonymity, but, to achieve this goal, they have ignored the effect of side information (Ma, C. Y., Yau, D. K., Yip, N. K., & Rao, N. S., 2013) while achieving the anonymity. With the help of side information like query probability of user and other information, an invader can easily identify at least some of the dummy locations that were added by the user to keep himself anonymous. Although some researchers have proposed solutions to address these problems, even then it is difficult to cope with this issue because of the associated high communication and storage cost.

Caching-based privacy enhancement technique has been used by many other researchers in the past. They have used different techniques to send queries to the location-based servers, but, to avoid the servers, they have used caching mechanism. Authors in (Amini et al., 2011) also proposed a caching based mechanism to deal with the privacy issue. They have proposed, that in order to get the spatial information for a moving object, they may fetch the required information before the arrival of the moving object in that area. In this way, even if an adversary has accessed the server data, he may not be able to get the information because the time when the user sent the query to the server, he was not in that region. The advantage of this approach is, that before entering that area, the user had all the required information and now for any query, he may search for it locally within his own device. The disadvantage of this approach is that the user has to store a large amount of data on his own device and the device must run the computations.

In MobiCrowd (Shokri, R., Theodorakopoulos, G., Papadimitratos, P., Kazemi, E., & Hubaux, J. P., 2014), a new idea was proposed that the spatial information required by a user may be provided by the others present in the same area. In this method, before sending a query to the location-based server, user sends a query to the other mobile nodes present in the vicinity. In case he receive the required information from any of the existing pair, he has no need to send the query to the location-base server. The risk of sending personal information to an untrusted server has been reduced this way. This scheme is good but practically it is not very useful. It is not possible to receive a response whenever a user sends a query to his neighbor. So ultimately, he has to send the query to the server but no solution has been provided for this scenario. Since this method deals with the peers in the same area, it has no proper caching mechanism and so the cache hit rate of this method is very low.

In (Zhu et al., 2013), authors have proposed a caching-based method to provide a solution. According to them, whenever a user sends a query to the location-based server, he need to cache data that is not yet present in cache. This way they keep on adding more and more data to the cache. This works fine but the problem is that they did not consider the importance of side information when contacting the location-based server. It is possible that when a user searches the cache and does not find any relevant information and contacts the server, he is trapped. This is because the adversary may get information about the user by examining the side information. Another problem is that they did not define a privacy metric for the measurement of effect of caching on privacy.

In (Niu et al., 2014), authors have proposed a dummy location selection algorithm that defines the way to select dummies for the purpose of anonymity and in this way they have achieved the privacy for the users. They also have considered the concept of side information and their proposed algorithm selects dummies considering the effect of side information. But they did not provide the way to cache the data and like many other methods provided a solution for the problem of sending information to the location-based server.

In (Gedik, B., & Liu, L., 2004), authors have used the concept of trusted base-stations. Any user who wants to contact the location-based server, first needs to send the query to the base-station and then the base stations will send the query to the location-based server. This is a distributed approach in which each base-station has a coverage area and all the moving objects inside that area will send query to the base-station. This approach is supposed to be more efficient and reliable than the other centralized approaches because it has many advantages like scalability, and less chances of failure due to distributed load on base-stations. There is also the low probability of bottleneck problem that may arise when large number of users start sending queries to the server. Although this approach does not directly access the privacy issue, but logically user data sent through this method is less prone to attacks because there are multiple base-stations who receive the queries from the users and forward them to the location-based server. When the user leaves one base-station's coverage area and enters

the region covered by the other base-station, it has to contact the new base-station and this way it is difficult for an invader to identify him.

Yi et al. in (Yi et al., 2014) proposed the idea of view field nearest neighbor query. In their proposed method, they have addressed the objects that fall within the view field of an object. According to them, for a moving object it is important to keep track of the objects that fall within that specific area. They also have defied the different view field areas of different objects. For a person it is normally 950 whereas it is about 1100 for an iPhone (Apple, http://www.apple.com/iphone/). Using the view field concept, the authors have discussed the k-nearest neighbors within the user's primitives. They also have used the grid index for the indexing of data set. The whole process in this method has been divided into two major sections. In the first section, they have described in details the naïve exploration algorithm that divides the area in conceptual partitions and then uses them. In second section, named in their discussion as update phase, they have proposed a monitoring technique that monitors the movement of data objects.

3. Trusted Base Stations-Based Privacy Preserving Technique in Location-Based Services

In this paper we have proposed a method to ensure the privacy of the users who use the location-based services by sending queries to untrusted servers. We have used the same approach presented in (Niu et al., 2015) in the way that we have used the concept of caching the data and use of k-anonymity approach while sending the queries to the location-based server. But our caching mechanism and the criteria to select the dummies is totally different from the approach used by the authors in that paper. In the following sub-sections we will describe both parts of our proposed method in detail and will explain how our approach is different and better than the approach used in (Niu et al., 2015).

3.1 An Overview of the Proposed Model

As mentioned earlier in this paper, we are using the concept of caching the data in conjunction with k-anonymity. Both, the caching of data on caching server and the use of k-anonymity is used to improve the privacy of the user. In case of caching, it is achieved by sending query to the cache server instead of location-based server. If the required results are available in the cached data, it will be returned to the user and hence privacy is achieved by not contacting the location-based server. On the other hand, if the required information is not available in cached data, then the user's query will be sent to the location-based server. To achieve the privacy in this case, we send

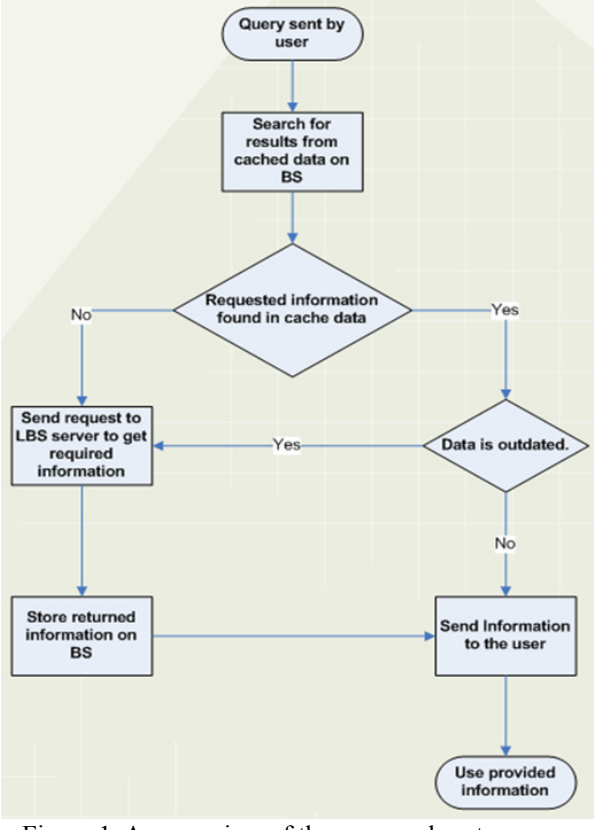

Figure 1. An overview of the proposed system

k-1 dummy locations with the actual user's location to make it k-anonymous. In this case, if even the security of location-based server has been compromised, it is very difficult to identify the actual user due to two reasons. One, the actual user was k-anonymous and two, as he is not frequently sending queries to location-based server, as such, it is not an easy task to identify it by simple approaches like statistical analysis etc. Flow chart shown below in Figure 1, shows the complete structure and functionality of the system and gives a complete overview of the proposed method.

3.2 Data Caching on Caching Server

To the best of our knowledge, for the first time, we are using caching servers to cache data. We have used a distribute approach to communicate with the location-based server and have used the concept of trusted base-stations. There are many base-stations connected to the location-based server. Each base-station has a pre-defined coverage area and it acts as a caching server. All the objects that are moving within its coverage area can send queries to him and in response, it will send back the available information.

As shown in Figure 2, there is one location-based server for the whole region. In that region, there are multiple base-stations that are connected to that server and each of them has its own coverage area. It is very important that these base-stations are not the Wireless LAN Access Points (APs).

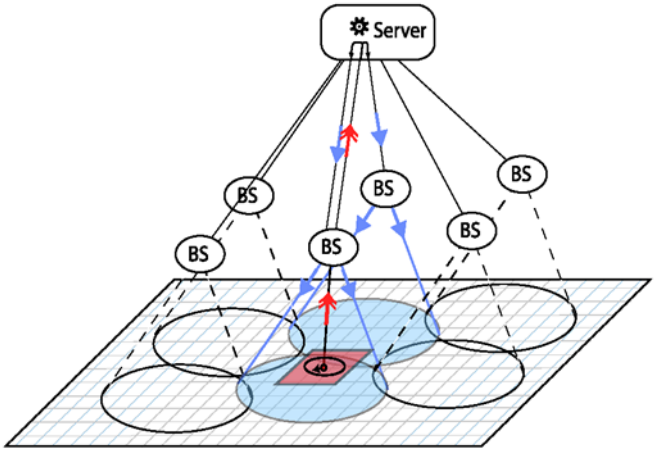

Figure 2. Base-stations for caching (Gedik, B., & Liu, L., 2004)

In previous work, APs were used to cache the data but they have a very limited storage capacity. In case there were no APs, data was stored on mobile devices which make that solution impractical. In our case, base-stations are acting as the caching servers with a wide coverage area and they can store a large amount of data. Due to wide coverage area and more storage capacity, this solution is not limited to a specific area or for pedestrians moving around in streets but it also deals with other mobile objects like cars moving on roads etc.

3.3 Achievement of K-Anonymity

To achieve k-anonymity, we have proposed an algorithm that selects the dummies to make a user k-anonymous. For the selection of dummies, we have considered many factors that help to identify the best suitable for this purpose. Their selection is an important factor that not only help to hide the user's identity from the location-based server but also helps to improve the cache hit ratio. Dummies selected form the area relevant to the user, adds the information to the cache data that are relevant to the user and hence, increase the probability that a user may get the relevant information from the cached data.

As part of dummy selection process, we first calculate the user's moving path. ie. his trajectory. We are considering that if a user is heading towards south, dummies located in the north are not useful for him. So we can simply ignore them. Second, to narrow down the relevant area of interest, we define the sector size. This is also an important factor because, for example, if the user is passing through a crowded area, then we can decrease the sector size because in big sector, he may find too many relevant information and it may make it difficult for him to select the best suitable information. Instead, if he is passing through the desert, he may need to increase the sector size to get some useful information. After defining an appropriate sector size, a sector is defined along the user's trajectory. Now, at this stage, we have defined the area that is suitable for the user to get

better results from both, the caching server and the dummies. Now we will select the dummies that have the same query probability as the user and will select k-1 dummies from them at random. This will return the set of k-1 selected dummies. Figure 3 shows a scenario where dummies are selected using the above mentioned process.

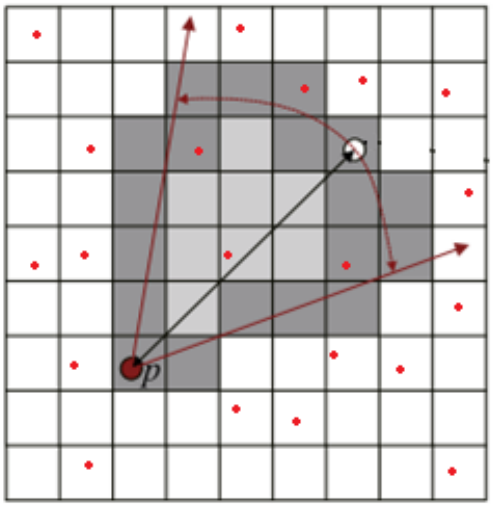

Figure 3. The process of dummies selection for k-anonymity

3.4 Calculation of User'S Trajectory

Let the user is moving along the path as shown in Figure 4 with dotted line that give us the locus of his path. Let u $\vec{}$ be the unit vector along this path. Then we can calculate the directional derivative $\nabla_u f(x_0, y_0, z_0)$ that give us the rate of change or the rate at which the function $f(x, y, z)$ changes at a point (x_0, y_0, z_0) in the direction of $\vec{u}$. It is the vector form of the usual derivative and could be defined as

$$\nabla_u f = \nabla_f . \frac{u}{|u|} \tag{1}$$

Now by the definition, we can write ∇ in the following way.

$$\vec{\nabla} = \left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right).$$

In addition, the unit vector in the direction of $\vec{u}$ could be defined as:

$$\hat{u} = \frac{\vec{u}}{|\vec{u}|} \tag{2}$$

Unit vector always represents the direction.

Now from both equations 1 and 2.

$$\vec{\nabla} f = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}\right)$$

Also as $\hat{u}$is the unit vector, so we can get data points or set of vectors in the direction of u.

Hence,

$$\nabla_u f = \frac{\partial f}{\partial x} u_x + \frac{\partial f}{\partial y} u_y + \frac{\partial f}{\partial z} u_z$$

So basically, user gives the path in form of data points and we calculated the change with respect to its coordinates, x, y, z. After that, it calculates the dot product that returns a scalar value which tells us the amount of data which match in the direction of reference value.

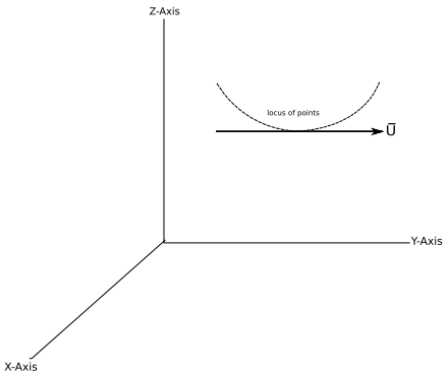

Figure 4. Calculation of directional vector

4. Performance Evaluation

In this section we have presented the results obtained by running the simulation setup built using the Riverbed Simulation Modeler (Riverbed Simulation Modeler, http://www.riverbed.com/). Our setup includes a location-based services server and multiple number of base-stations as it was shown in proposed model section. The cache servers used to cache data have been used as the base-stations in this approach. These servers redirect the user request to the location-based server if they find that relevant data is not stored in them. Mobile-stations (available in Riverbed simulator) have been used as the moving devices. Along with these, iPhones have also been used as the mobile agents.

Figure 5, shows the cache hit ratio. This shows how many user's queries were addressed by the cache servers. It is clear from the graph that in start this rate was zero. But after that, when the data was queried and in response, it was stored in the cache server, the cache hit rate was increased. This is because that user was moving in a path and he was selecting the dummies that were close to his path as well. So when he sent the query to the location-based server, it mean actually 10 queries were sent to the server and the data returned by the server was stored in the cache server. So in response to his query, 10 similar queries providing information relevant to his path were stored in the cache.

Figure 6, shows the amount of data sent and received by the users. It shows huge amount of data sent by the users to the cache server and the location-based server. Due to lack of space we are presenting only one graph of user traffic because the amount sent and received by the user was almost the same.

Figure 7, show the traffic sent by the server to the client. Small amount of data trasfer between the user and the server shows that most of the queries were addressed by the caching servers and the required information was provided to the users by the caching servers. In those cases, users requests were not forwarded to the server. This was the main purpose to use caching servers. As the users queries will be addressed by the caching servers, small number of queries will be sent to the location-based servers and in response it will enhance the privacy of the users. Furthermore, as we have used the concept of base-stations instead of APs, they have now a very big coverage area and a large amount of storage capacity as compared to the APs.

Figure 8, shows the difference between the traffic sent/received by the user and the location-based server. Due to the use of caching, there is a clear difference between the data traffic between these two entities of the system. As compared to other solutions (Niu et al., 2015), our proposed solutions showed good results because it focused on the selection of dummies as well and selected only those which were lying along the user's trajectory. This not only improved the dummy selection process, but also improved the cache hit rate, and in response, there is a clear difference between the user and the server's data traffic.

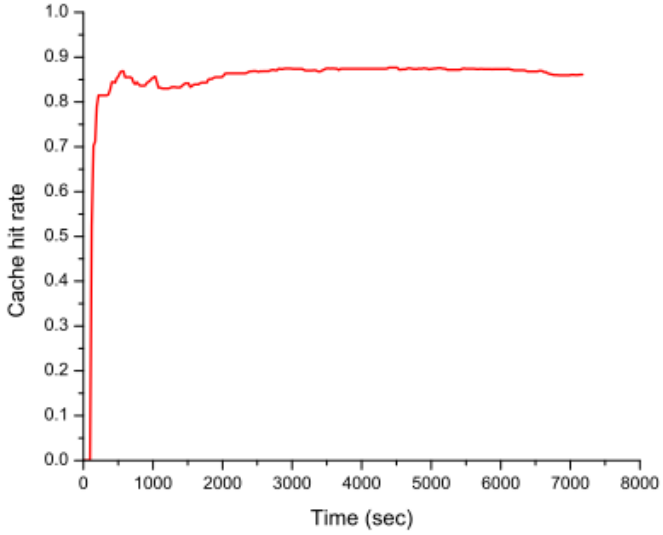

Figure 5. Cache hit rate in two hours with fixed number of dummies

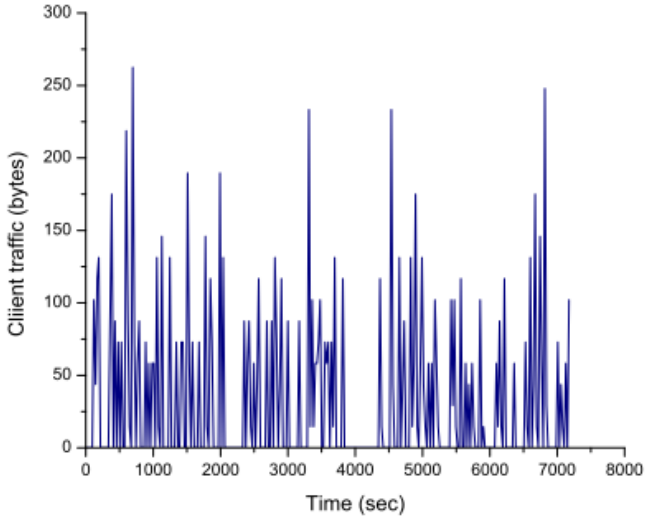

Figure 6. Data sent and received by client nodes

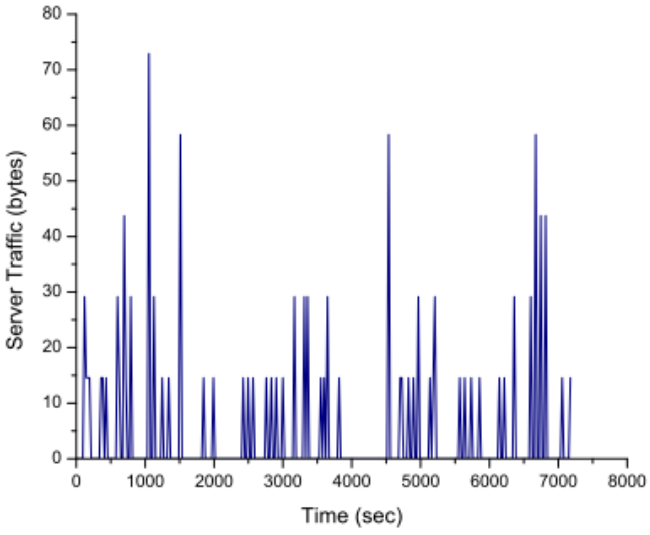

Figure 7. Data sent by servers in response to the user requests

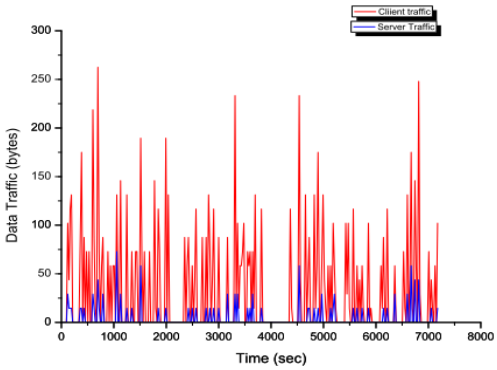

Figure 8. Comparison of data traffic between location-based services serve and the clients

5. Conclusion

In this paper we have proposed a method to enhance user's privacy when he contacts the location-based services server in order to get location information. We used a predefined approach, as it was already proposed by the others (Niu et al., 2015), but we used the concept of caching and k-anonymity and provided an efficient approach to deal with the privacy issue. In this method, our main concern was to select the dummies in such a way that they should not only help the user to make him anonymous but also the queries sent by those dummies should also be relevant to the user. And this could only be done, if we know the path along which the user is moving currently. In this case the dummies will retrieve the information about the places that the user visits, thus increasing the probability that the information will be more relevant to the user. Another important change we proposed is that we used caching servers instead of Aps along with storing the information within the users mobile devices. The drawback of old approaches was that APs have limited coverage area and storage capacity. It is also not feasible to store information on user devices because it adds more computational and saving complexities to user's devices and hence decreases the efficiency of those devices.

To the best of our knowledge, we are the first, who used caching servers for the purpose of caching data in loacation-based services.

References

Puttaswamy, K. P., Wang, S., Steinbauer, T., Agrawal, D., El Abbadi, A., Kruegel, C., & Zhao, B. Y. (2014). Preserving location privacy in geosocial applications. *Mobile Computing, IEEE Transactions on*, *13*(1), 159-173.

Shin, K. G., Ju, X., Chen, Z., & Hu, X. (2012). Privacy protection for users of location-based services. *Wireless Communications, IEEE*, *19*(1), 30-39.

Zhang, C., & Huang, Y. (2009). Cloaking locations for anonymous location based services: A hybrid approach. *GeoInformatica*, *13*(2), 159-182.

Ardagna, C. A., Cremonini, M., Damiani, E., Di Vimercati, S. D. C., & Samarati, P. (2007). Location privacy protection through obfuscation-based techniques. In *Data and Applications Security XXI* (pp. 47-60). Springer Berlin Heidelberg.

Yiu, M. L., Jensen, C. S., Møller, J., & Lu, H. (2011). Design and analysis of a ranking approach to private location-based services. *ACM Transactions on Database Systems (TODS)*, *36*(2), 10.

Mascetti, S., Freni, D., Bettini, C., Wang, X. S., & Jajodia, S. (2011). Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. *The VLDB Journal—The International Journal on Very Large Data Bases*, *20*(4), 541-566.

Marias, G. F., Delakouridis, C., Kazatzopoulos, L., & Georgiadis, P. (2005, June). Location privacy through secret sharing techniques. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a* (pp. 614-620). IEEE.

Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2015). Enhancing privacy through caching in location-based services. In *Proc. of IEEE INFOCOM*.

Gedik, B., & Liu, L. (2004). Mobieyes: Distributed processing of continuously moving queries on moving objects in a mobile system. In *Advances in Database Technology-EDBT 2004* (pp. 67-87). Springer Berlin Heidelberg.

Yi, S., Ryu, H., Son, J., & Chung, Y. D. (2014). View field nearest neighbor: A novel type of spatial queries. *Information Sciences*, *275*, 68-82.

Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J. P., & Aad, I. (2011, January). Privacy in mobile computing for location-sharing-based services. In*Privacy Enhancing Technologies* (pp. 77-96). Springer Berlin Heidelberg.

Pingley, A., Zhang, N., Fu, X., Choi, H. A., Subramaniam, S., & Zhao, W. (2011, April). Protection of query privacy for continuous location based services. In *INFOCOM, 2011 Proceedings IEEE* (pp. 1710-1718). IEEE.

Ma, C. Y., Yau, D. K., Yip, N. K., & Rao, N. S. (2013). Privacy vulnerability of published anonymous mobility traces. *Networking, IEEE/ACM Transactions on*, *21*(3), 720-733.

Amini, S., Lindqvist, J., Hong, J., Lin, J., Toch, E., & Sadeh, N. (2011, June). Caché: caching location-enhanced content to improve user privacy. In*Proceedings of the 9th international conference on Mobile systems, applications, and services* (pp. 197-210). ACM.

Shokri, R., Theodorakopoulos, G., Papadimitratos, P., Kazemi, E., & Hubaux, J. P. (2014). Hiding in the mobile crowd: Locationprivacy through collaboration. *Dependable and Secure Computing, IEEE Transactions on*, *11*(3), 266-279.

Gruteser, M., & Grunwald, D. (2003, May). Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services* (pp. 31-42). ACM.

Cheng, R., Zhang, Y., Bertino, E., & Prabhakar, S. (2006, January). Preserving user location privacy in mobile data management infrastructures. In *Privacy Enhancing Technologies* (pp. 393-412). Springer Berlin Heidelberg.

Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on* (pp. 106-115). IEEE.

Mokbel, M. F. (2007, May). Privacy in Location-based Services: State-of-the-art and Research Directions. In *Mobile Data Management, 2007 International Conference on* (pp. 228-228). IEEE.

Bamba, B., Liu, L., Pesti, P., & Wang, T. (2008, April). Supporting anonymous location queries in mobile environments with privacygrid. In *Proceedings of the 17th international conference on World Wide Web* (pp. 237-246). ACM.

Hu, H., & Xu, J. (2009, March). Non-exposure location anonymity. In *Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on* (pp. 1120-1131). IEEE.

Pingley, A., Yu, W., Zhang, N., Fu, X., & Zhao, W. (2009, June). Cap: A context-aware privacy protection system for location-based services. In*Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on* (pp. 49-57). IEEE.

Zhu, Z., & Cao, G. (2011, April). Applaus: A privacy-preserving location proof updating system for location-based services. In *INFOCOM, 2011 Proceedings IEEE* (pp. 1889-1897). IEEE.

Li, Q., & Cao, G. (2013, January). Efficient privacy-preserving stream aggregation in mobile sensing with low aggregation error. In *Privacy Enhancing Technologies* (pp. 60-81). Springer Berlin Heidelberg.

Zhu, X., Chi, H., Niu, B., Zhang, W., Li, Z., & Li, H. (2013, December). Mobicache: When k-anonymity meets cache. In *Global Communications Conference (GLOBECOM), 2013 IEEE* (pp. 820-825). IEEE.

Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2014, April). Achieving k-anonymity in privacy-aware location-based services. In *INFOCOM, 2014 Proceedings IEEE* (pp. 754-762). IEEE.

Web References

http://www.apple.com/iphone/, "iPhone," Apple. Retrieved May 25, 2015, from http://www.apple.com/iphone/

Riverbed. "Riverbed Simulation Modeler," Riverbed. Retrieved May 16, 2015, from http://www.riverbed.com/