ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Continuous Location Based Service for User Defined Grid Structure Providing Semi Trusted Third Party

[1] K.Indumathi,[2] R.Janci,[3] J.Jenifa, [4]J.Jenifer, [5]S.Kaviya

[1]Assistant Professor,[2,3,4] UG Scholars, Department of Information Technology
Kings Engineering College, Chennai,India
[2]janci.lingam@yahoo.com,[3]jenifajoseph03@gmail.com,[4]josephkennady31@gmail.com,[5]kaviyarishi2@gmail.com.

Abstract – **Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. Unfortunately, existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. we propose a user-defined privacy grid system called dynamic grid structure (DGS); the first holistic system for privacy-preserving snapshot and continuous LBS. In this grid structure only requires semitrusted third party termed *query server* (QS), between the user and the service provider (SP). QS only needs to be semi-trusted because it will not collect/store or even have access to any userlocation information.**

I. INTRODUCTION

IN today's world of mobility and ever-present Internet connectivity, an increasing number of people use location-based services (LBS) to request information relevant to their current locations from a variety of service providers (SPs). This can be the searc]h for nearby points of interest (POIs) (e.g., restaurants and hotels), location-aware advertising by companies, traffic information tailored to the highway and direction a user is traveling and so forth. The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be willing to disclose. By tracking the requests of a person it is possible to build a movement profile which can reveal information about a user's work (office location), medical records (visit to specialist clinics), political views (attending political events), etc. Nevertheless, LBS can be very valuable and as such users should be able to make use of them without having to give up their location privacy. A number of approaches have recently been proposed for preserving the user location privacy in LBS. In general, these approaches can be classified into two main categories. (1) Fully-trusted third party (TTP).

The most popular privacy-preserving techniques require a TTP to be placed between the user and the service provider to hide the user's location information from the service provider. The main task of the third party is keeping track of the exact location of all users and blurring a querying user's location into a cloaked area that includes k _ 1 other users to achieve k-anonymity. This TTP model has three drawbacks. (a) All users have to continuously report their exact location to the third party,even though they do not subscribe to any LBS. (b) As the third party knows the exact location of every user, it becomes an attractive target for attackers. (c) The k-anonymity- based techniques only achieve low regional location privacy because cloaking a region to include k users in practice usually results in small cloaking areas. (2) Private information retrieval (PIR) or oblivious transfer (OT). Although PIR or OT techniques do not require a third party, they incur a much higher communication overhead between the user and the service provider, requiring the transmission of much more information than the user actually needs Only a few privacy-preserving techniques have been proposed for continuous LBS.These techniques rely on a TTP to continuously expand a cloaked area to include the initially assigned k users. These techniques not only inherit the drawbacks of the TTP model, but they also have query processing overhead Since the other limitations.(1)Inefficiency.Continuously expanding cloaked areas substantially increases the database server receives a set of consecutive cloaked areas of a user at different timestamps, the correlation among the cloaked areas would provide useful information for inferring the user's location. . (2) Privacy leakage. (3) Service termination. A user has to terminate the service when

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

users initially assigned to her cloaked area leave the system.

II EXISTING SYSTEM

A number of approaches have recently been proposed for preserving the user location privacy in LBS.]]In general, these approaches can be classified into two main categories.

1. **Fully-trusted third party (TTP)** requires a TTP to be placed between the user and the service provider to hide the user's location information from the service provider. The main task of the third party is keeping track of the exact location of all users and blurring a querying user's location into a cloaked area that includes k _ 1 other users to achieve k-anonymity.

Drawbacks:

(a) All users have to continuously report their exact location to the third party, even though they do not subscribe to any LBS.

(b) As the third party knows the exact location of every user, it becomes an attractive target for attackers.

(c) The k-anonymity- based techniques only achieve low regional location privacy because cloaking a region to include k users in practice usually results in small cloaking areas.

2. **Private information retrieval (PIR)** or **oblivious transfer (OT)** techniques do not require a third party, they incur a much higher communication overhead between the user and the service provider, requiring the transmission of much more information than the user actually needs.

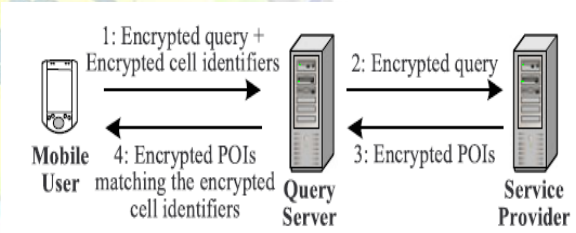
3. **Continuous LBS** rely on a TTP to continuously expand a cloaked area to include the initially assigned k users.

Drawbacks:

(1) Inefficiency. Continuously expanding cloaked areas substantially increases the query processing overhead.

(2) Privacy leakage. Since the database server receives a set of consecutive cloaked areas of a user at different timestamps, the correlation among the cloaked areas would provide useful information for inferring the user's location.

(3) Service termination. A user has to terminate the service when users initially assigned to her cloaked area leave the system.



III. RELATED WORKS

Spatial cloaking techniques have been widely used to peserveuser location privacy in LBS. Most of the existing spatial cloaking techniques rely on a fully-trusted third party (TTP), usually termed *location anonymizer*, that is required between the user and theservice provider . When a user subscribes to LBS, the location anonymizer will blur the user's exact location into a cloaked area such that the cloaked area includes at least k –1 other users to satisfy k-anonymity. The TTP model has four major drawbacks. (a) It is difficult to find a third party that can be fully trusted. (b) All users need to continuously update their locations with the location anonymizer, even when they are not subscribed to any LBS, so that the environments, these techniques still rely on the k-anonymity privacy requirement and can only achieveregional location privacy. Furthermore, these techniques require users to trust each other, as they have to reveal their locations to other peers and rely on other peers' locations to blur their locations. In another distributed method was proposed that does not require users to trust each other, but it still uses multiple TTPs. Another family of algorithms uses incremental nearest neighbor queries, where a query starts at an "anchor" location which is different from the real location of a user and iteratively retrieves more points of interest until the query is satisfied . While it does not require a trusted third party, the approximate location of a user can still be learned; hence only regional location privacy is achieved. Cryptographic tools were used to protect outsourcing data. An order-preserving encryption scheme uses a bucket-based encryption E such that $E(x) < E(y)$ for every pair of values for which $x < y$. However, there does not seem to be a straightforward

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

way to extend it to protect spatial

location anonymizer has enough information to compute cloaked areas. (c) Because the location anonymizer stores the exact location information of all users, compromising the location anonymizer exposes their locations. (d) k-anonymity typically reveals the approximate location of a user and the location privacy depends on the user distribution. In a system with such *regional location privacy* it is difficult for the user to specify personalized privacy requirements. The feeling based approach alleviates this issue by finding a cloaked area based on the number of its visitors that is at least as popular as the user's specified public region. Although some spatial clocking techniques can be applied to peer-to-peer data. Anotherapproach described in for outsourcing data uses homomorphicencryption to enable aggregate SQL queries over encrypted databases. The scope focuses only on simple numerical domains and aggregate queries in SQL. This approach has also been shown to be insecure in . For spatial data, another family of privacy-preserving techniques uses cryptographic tools such as private information retrieval (PIR) or oblivious transfer (OT). PIR allows a user to retrieve a POI from a database without the server knowing which POI was retrieved. OT has the additional property that the user only learns the requested POI and does not learn anything about any other POI. Ghinita et al. proposed a PIR-based scheme which eliminates the trusted location anonymizer. Their work uses a PIR matrix with n POIs in total and size t × t with t = ⌈√n⌉. Using PIR a user can retrieve POIs only columnwise, corresponding to O(√n) POIs for each request. This is significantly more expensive than just retrieving the O(1) relevant POIs. Their experimental results show that the communication overhead of their scheme is much higher than that of using the TTP model.proposed to use a two-level combination of PIR and OT . First, a user selects the appropriate column in a grid using PIR and then uses OT to retrieve the exact grid cell. Their approach focuses on protecting the data of the database system by allowing the user to only learn the POIs in the current grid cell of the user. Because of the nature of PIR, however, the user still needs to receive the whole column (and thus O(√n) points of interest). A scheme proposed in uses OT to hide users' locations from a service provider while enabling a payment infrastructure, but the scheme still requires a proxy as a TTP. Also studied for privacy in LBS are methods which work on encrypted or transformed data. For example, Khoshgozaran and Shahabi proposed a system which uses Hilbert curves to map locations into a different space and then solves NN queries in the transformed space . A similar approach but using encryption Their work focuses on outsourcing a database in encrypted format to a service provider and allows users to perform k-NN queries on the encrypted database. Their focus, however, is more on protecting the database instead of the privacy of the users. A few privacy-preserving techniques have attempted to use the TTP model for continuous LBS The idea of is to keep expanding an initial cloaked area to include at least the same k users, is to predict a user's footprints and blur each footprint into a k-anonymized area, and is to use a mix-zone to make the users located in there at the same time indistinguishable. The TTP model has been extended to protect the privacy of ananonymized group of users by generalizing their spatial query regions to make their queries indistinguishable and guarantee that the number of their requested service values is at least mto achieve m-invariance. Temporal cloaking and encryption techniques are used for aggregate traffic data collection butthey cannot provide privacy-preserving continuous LBS.Another technique proposed to protect continuous LBS is using dummy queries together with a real query However, this technique issues more queries than the user really needs. In our system a user never transmits actual location information (apart from the query area, which is only seen by the service provider and which can be chosen arbitrarily large), and the type of POI in a query can only be read by the service provider. The query server has even less information available, it does not knowthe query area nor the type of POI searched. Christo Ananth et al. [2] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to destination.

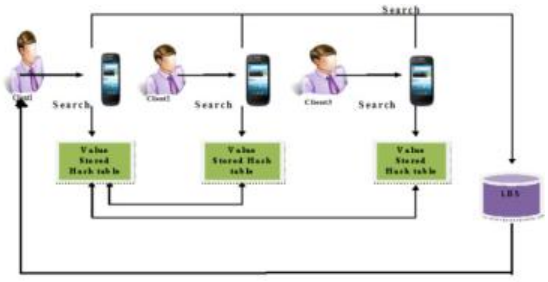
Disadvantages:

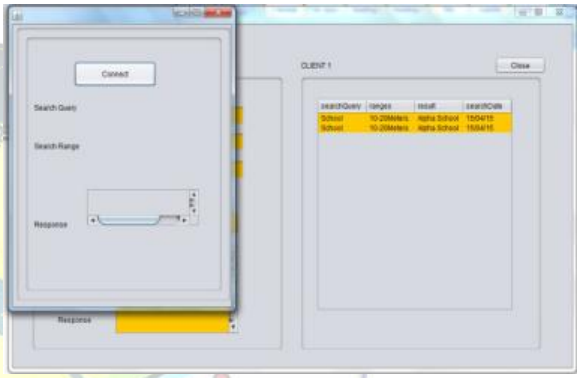
i. Can be inferred from a user's whereabouts. This could make user the target of blackmail or harassment.
ii. A stalker can also exploit the location information.
iii. Misuse their rich data by, e.g., selling it to advertisers or to private investigators.

iv. Continuous location report by all users
v. Attracted by hacker
vi. low regional location privacy.

IV. PROPOSED SYSTEM

We propose a user-defined privacy grid system called dynamic grid system (DGS) to provide privacy- preserving snapshot and continuous LBS. The main idea is to place a semi-trusted third party, termed query server (QS), between the user and the service provider. QS only needs to be semi-trusted because it will not collect store or even have access to any user location information. Semi-trusted in this context means that while QS will try to determine the location of a user, it still correctly carries out the simple matching operations required in the protocol, i.e., it does not modify or drop messages or create new messages. An untrusted QS would arbitrarily modify and drop messages as well as inject fake messages, which is why our system depends on a semitrustedQS.





V MODULES

1) Client Creation
2) Search query
3) Retrieve peer values
4) LBS Module

5.3.1 Modules

Client Creation

In this module explains the client parts in the project. There are different kind of user's in our project. The user may register for the various purpose. Location-based services can be queried by users to provide real-time information related to the current position and surroundings of the device, e.g., contextual data about points of interest such as petrol stations, or more dynamic information such as traffic

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

conditions. The value of LBSs is in their ability to obtain on the fly up-to-date information.

Search query

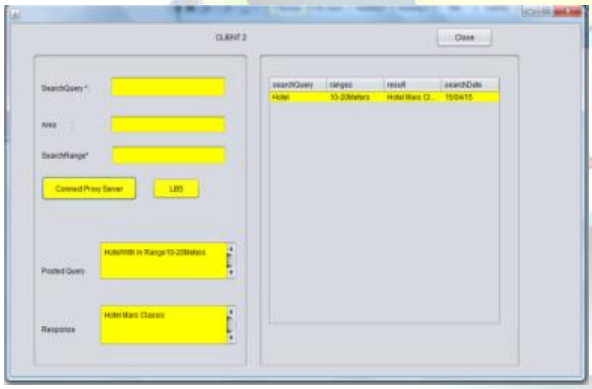
Each time an LBS query is submitted, private information is revealed. Users can be linked to their locations, and multiple pieces of such information can be linked together. They can then be profiled, which leads to unsolicited targeted advertisements or price discrimination. After add the clients, he/she may give the query to search. Results will be executed.

Retrieve peer values

In this module explains the peer values of the client. If the searched query results are not in the result set, then it will search the results in the peer values. If the results are in the peer set values the it will take the peer value for the final result.

LBS Module

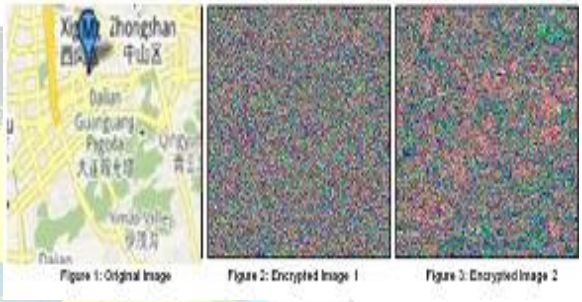
In the searched query results are not obtained in the result set, then it will search the results in the database based on the LBS technique. The results are retrieved from the database.



LBS Search Query:

ALGORITHM (Chaotic Mapping)

Image encryption algorithm is proposed based on combination of pixel shuffling and three chaotic maps. This algorithm is based on pixel scrambling where in the randomness of the chaos is utilized to scramble the position of the data. Shuffling is used to expand diffusion in the image and dissipate the high correlation among image pixels. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. In the proposed algorithm, the plainimageis first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out. After that the shuffled image is encrypted using chaotic sequence generated by one another chaotic map. In order to evaluate performance, the proposed algorithm was measured through a series of tests. Experimental results illustrate that the scheme is highly key sensitive and shows a good resistance against brute-force and statistical attacks.



we describe all the steps for encryption and decryption of the imageusing both chaotic logistic maps. Complete process is described in the following **steps**:The encryption process uses an 80 bit external secret key, the key is divided into blocks of 8-bit each, called session keys. Session keys referred as:
K = k1k2…..k20 (in hexadecimal),(1)

Here, ki's are alphanumeric characters. Thus, each group of two alphanumericcharacters represents a session key.We use following two logistic maps for encryption

Xn+1 = 3.9999Xn (1-Xn), (2)
Yn+1 = 3.9999Yn (1-Yn),(3)

A New Algorithm of Encryption and Decryption of Images 743.Using these logistic maps initial conditions for each logistic map, namely (X0 Here ki's are parts of secret key in hexadecimal mode as explained in equation 1 Now initial condition X0 is calculated as:

X0 = (X01 + X02) mod 1(6)

Similarly, we calculate the initial condition Y0 for the second logistic map,

Y01 = (B2)10/224 ,7)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Where B is the binary string of session keys. And

Y02 = (B2 [P1] x 20 + B2 [P2] x 21 + B2 [P3] x 22 +……..+ B2 [P24] x 223) / 224, (7)

And

Y0 = (Y01 + Y02) mod 1, (1

Next step is to read three consecutive bytes, these three bytes represent the value of red, green and blue (RGB) color respectively. Then we perform encryption on first 16 bits of the image using the following formula:

andY0) are calculated.X0 is calculated using X01 and X02 where:X01 is binary representation of three blocks of session keys e.g. K4K5K6.

X01 = (K41 x 20 + K42 x 21 + …. + K61 x 216 + K62 x 217 + ….+ K68 x 223) / 224,(4)

X02 = ((k13)10 + (k14)10 + (k15)10 + … + (k18)10) / 96,(5)

Here ki's are parts of secret key in hexadecimal mode as explained in equation 1 Now initial condition X0 is calculated as:

X0 = (X01 + X02) mod 1(6)

Conclusion:

We have proposed a novel approach to enhance the privacy of LBS users, to be used against service providers who could extract information from their LBS queries and misuse it. We have developed and evaluated MobiCrowd, a scheme that enables LBS users to hide in the crowd and to reduce their exposure while they continue to receive the location context information they need. MobiCrowd achieves this by relying on the collaboration between users, who have the incentive and the capability to safeguard their privacy. We have proposed a novel analytical framework to quantify location privacy of our distributed protocol. Our epidemic model captures the hiding probability for user locations, i.e.,the fraction of times when, due to MobiCrowd, the adversary does not observe user queries. By relying on this model, our Bayesian inference attack estimates the location of users when they hide. Our extensive joint epidemic/ Bayesian analysis shows a significant improvement thanks to MobiCrowd, across both the individual and the average mobility prior knowledge scenarios for the adversary. We have demonstrated the resource efficiency of MobiCrowd by implementing it in portable devices.

Next step is to read three consecutive bytes, these three bytes represent the value of red, green and blue (RGB) color respectively. Then we perform encryption on first 16 bits of the image using the following formula:

((R)10 + (K4)10 + (K5)10) mod 256, ((G)10 + (K5)10 + (K6)10)mod 256,((B)10 + (K6)10 + (K4)10) mod 1 , (8)

After encryption of the 16 bit block, we modify the session key using the formula:

(Ki)10 = ((Ki)10 + (K10)10) mod 256,(1≤ i ≤ 9).

Future Enhancements : Techniques proposed to protect location privacy in LBSs can be classified based on how they distort the users' queries before the queries reach the LBS server. Queries can also be camouflaged by adding some *dummy queries*, or be completely eliminated and *hidden* from the LBS. Combinations of these methods have been employed in the existing (centralized or distributed) mechanisms. We now discuss these approaches in more detail. In the *Baseline* scenario, we compute privacy against the inference attack, assuming that the adversary ignores his LBS observations and relies only on his background knowledge.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in Proc. 17th Int. Conf. World Wide Web, 2008, pp. 237–246

.[2] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

.

[3] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Trans.MobileComput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

[4] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in Proc. 1st Int. Conf. Mobile Syst., Appl. Services, 2003, pp. 31–42.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D.Papadias,"Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proc. 32nd Int. Conf. Very Large Data Bases, 2006, pp. 763–774.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

[7] T. Xu and Y. Cai, "Location anonymity in continuous locationbased services," in Proc. 15th Annu.ACM Int. Symp. Adv. Geographic Inf. Syst., 2007, pp. 39:1–39:8.

[8] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services," in Proc. IEEE INFOCOM, 2008, pp. 547–555.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,"Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD Int. Conf. Manag. Data, 2008,pp. 121–132.

[10] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Location-based services with a payment broker," in Proc. 7th Int. Conf. Privacy Enhancing Technol., 2007, pp. 77–94.

[11] R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries," in Proc. IEEE Int. Conf. Intell. Security Informat., 2009, pp. 149–154.

[12] J. M. Kang, M. F. Mokbel, S.Shekhar, T. Xia, and D. Zhang, "Continuous evaluation of monochromatic and bichromaticreverse nearest neighbors," in Proc. IEEE 23rd Int. Conf. Data Eng., 2007, pp. 806–815.

[13] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in Proc. IEEE Int. Conf. Data Eng., 2006, p. 71.

[14] S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in Proc. 10th Int. Conf. Mobile Data Manag.: Syst. Services Middelware, 2009, pp. 443–448
.

[15] W. B. Allshouse, W. B. Allshousea, M. K. Fitchb, K. H. Hamptonb, D. C. Gesinkc, I. A. Dohertyd, P. A. Leonebd, M. L. Serrea, and
W. C. Millerb, "Geomasking sensitive health data and privacy protection: An evaluation using an E911 database," Geocarto Int., vol. 25, pp. 443–452, Oct. 2010.

[16] A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing kanonymityin location based services," SIGKDD Explor.Newsl.,vol. 12, pp. 3–10, Nov. 2010.

[17] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, pp. 213–229.

[18] A. Menezes, M. Qu, and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication," in Proc. Workshop Selected Areas Cryptography, 1995, pp. 22–32.

[19] S. Yau and H.An, "Anonymous service usage and payment in service-based systems," in Proc. IEEE 13th Int. Conf. High Perform.Comput.Commun., 2011, pp. 714–720.

[20] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian,"Where's that phone?: Geolocatingip addresses on 3G networks,"
in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf., 2009,pp. 294–300.