International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Discovering the Optimal Meeting Place for the Protection of Privacy of Mobile Device Users Using Privacy Preserving Algorithm

Parameswari.T1#& T.Sreekanth#2

[1]PG Scholar, Department of Computer Science and Engineering, Malineni lakshmaiah Engineering College, S.Konda, Prakasam D.t., India.
parameswarituraka@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Malineni lakshmaiah Engineering College, S.Konda, Prakasam D.t., India.
sreekanth.thullibilli@gmail.com

ABSTRACT:

Now-a-days, people of urban and rural are using smart phones and mobile devices intensively. In particular urban population depends on the applications and gadgets which are provided by the mobile devices and smart phones to plan their daily life. The applications which are built on these devices mainly depend on the current or preferred locations of the user to provide the services they wish, which may cause damage to the privacy of mobile device users. In general no user wish to reveal their present location or the location they wish to go. In this paper, we proposed privacy preserving algorithms which will provide an optimal location for group of users.

KEYWORDS: Mobile devices; applications; privacy preserving

I.INTRODUCTION

In urban areas due to the rapid development of smart phone technology made the people to use location based services on their mobile devices. Advantage has been taken by the service providers by providing ever growing location based services for mobile device users. Millions of people are using location based services (LBS), to get information of particular location [1]. The two features that are popularly used based on location services are location check-ins and location sharing. Using location checking, user can share his/her current location to family, friends etc.., or user can obtain location specific information from third party service provider. The other LBS services provide the location sharing by the group or number of users also becoming popular now-a-days. Almost 20% of mobile users are using location sharing services according to recent survey [4]. One of the most popular applications of such type is taxi sharing application. By using such applications user current and preferred locations can be known by service provider which may leads to bad consequences on user's financial, social, business and political status.

User's current location and preferred locations should be kept secretly from other participant user and third party service provider which is an important aspect in such LSB applications. If such information like users and their availabilities [7], are de-anonymized to known the preferences. The third party service provider can identify the user location current and preferred location pairs easily if the user is using service provider application very often. Even third party service will track the user details to provide the quality service can indirectly harm the privacy of the user if the details are leaked in unauthorized way.

In this work, we focus on particular problem called Fair Rendez-Vous point problem which is an issue in LSBSs. By using the set of

user location preferences from the user, the FRVP problem will determine the location from the proposed location so that maximum distance between determined location and all the other preferred locations can be minimized that means it is fair to all users. Main goal of this paper is to provide privacy preserving practical techniques to solve the problem of FRVP, so that both the third party service provider and users who are participating cannot know locations of other users. Participating users can only know the optimal location.

We are going to solve the privacy problem of the user first by formulating the problem of FRVP as an problem of optimization, particularly the k-centre problem [12], and then privacy is provided among the participants with respect to one another and a third party service provider. Algorithms proposed by us will take the advantage of homomorphic properties of cryptosystems to compute an optimal fair rendez-vous point by using set of location preferences from the user. We provide an accurate analysis to show that our algorithms will not provide any way of guessing the participant preferred location. Including the theoretical analysis, we also made evaluation of practical efficiency and proposed algorithms performance by using the implementation of prototype on Nokia mobile device test beds. Finally we also propose the case of multi-preferences of the user based on priorities of location. We show the difference mainly in terms of performance and privacy, by using single preference case and initial experimental results are shown for the implementation of multi-preference.

II. RELATED WORK

The privacy preserving fair rendez-vous location has less or no attention in previous work. Authors Santos and Vaughn [21] discussed and presented a survey regarding meeting location algorithms and presented all related solutions for such problems. By considering aspects of user preference locations and constraints, the surveyed papers have not presented any privacy or security issues. Similarly, the proposed work of Berger et al. [22] presented meeting-location algorithm which is efficient and considers the time of two consecutive meetings.

In Secure Multiparty Computation (SMC) domain, several authors have presented privacy issues which are related to the computation of distance of two points [23] or routes [24]. There are also many results on research based on privacy preserving location problems. However, all the research results attempt to solve the mentioned problem in unique and different ways. Jaiswal and Nandi [25] proposed a platform of privacy preserving known as Trust No One, for locations which are located privately nearby points of interest.

Finally, the authors of paper [26], have proposed a simple architecture and evaluated the performance of different algorithms efficiently which made the privacy preserving of mobile device users easy by using two different algorithms.

III.SYSTEM DESIGN

We were considered a system with two major entities: (i) A group of users or mobile devices $U= \{u_1, u_2, \ldots, u_N\}$ and (ii) a third party service provider, which is known as Location Determination Server (LDS), which is source for computing the fair rendez-vous point or location from the group of user preferred locations. Each and every user can communicate with LDS by using some Internet connection.

Users can determine the coordinates $L_i=(x_i, y_i) \in N^2$ of their preferred location of rendez-vous location. We were considered a two-dimensional coordinate system. Users can mention the current or present location as rendez-

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

vous location or they can mention some preferred locations such as hotel etc.., away from present position.

We were defined the group of preferred rendez-vous locations of users as

$L= \{L_i\}^N_{i=1.}$

For simplicity, we use line_of_sight Euclidean distances between user preferred rendez-vous locations. All though actual real-world distance of two locations is at least as same as their Euclidean distance, the proportion between distances is assumed to be correlated with Euclidean respective distances.

To solve FRVP problem, we refer Privacy Preserving Fair Rendez-Vous Point (PPFRVP) algorithm. Generally, PPFRVP algorithm A accepts the inputs and generates the output, described below.

- Input: transformation *f* of preferred locations L_i: $f(L_1)||f(L2)||. . .||f(LN)$. Where *f* is nothing but secrete key based encryption function so that it is difficult to determine the input L_i without taking the help of the secrete key, by just observing $f(L_i)$.

- Output: an output $f(L_{fair})= g(f(L_1), f(L_2), . . . , f(L_N))$, where g is called as fairness function and $L_{fair}= (x1,y1) \in N^2$ is fair rendez-vous location so that it is difficult for the LDS to identify L fairby just knowing *f*(L fair).

  f(Lfair) is given, each and every user is capable to compute $Lfair= f^{-1}(f(Lfair))$ by using decryptionroutine and shared secrete key.

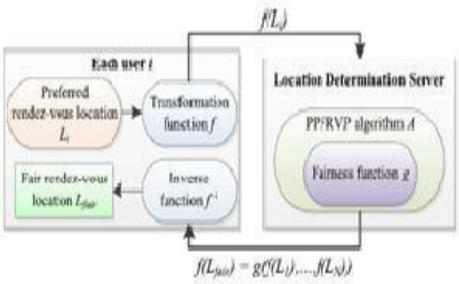

Fig. 1. Functional diagram of the PPFRVP protocol.

Fig. 1. Shown below describes the functional diagram of PPFRVP protocol, where LDS executes PPFRVP algorithm A. The fairness function g can be defined in different ways, based on the preferences of the policies or users.

The architecture for fair rendez-vous point determination by using privacy-preserving fair rendez-vous point is as shown below.

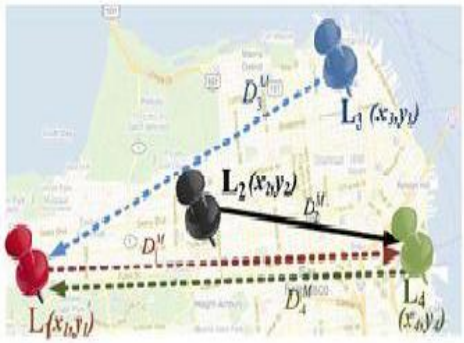

Fig. 2. PPFRVP scenario, where the fairness function is $g = \text{argmin}_i(D_i^M)$. The dashed arrows represent the maximum distance D_i^M from each user u_i to any user $j \neq i$, whereas the solid line is the minimum of all such maximum distances. The fair rendez-vous location is $L_{fair} = L_2 = (x_2, y_2)$.

Fig. 2 describes one such fairness function that reduces the maximum distance of any user to other locations. Function which is considered here is fair globally and can be extended easily to add additional parameters and constraints.

Flow Chart for Discovering the Optimal Meeting Location for the Protecting the privacy of Mobile Device Users is as shown in the following figure:

In the fig. 3, first the current and preferred locations are collected from the users.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

The collected locations are submitted to cryptosystem functions and a secrete key is combined with those inputs and stored in LDS. By retrieving inputs the PPFRVP algorithm A is going to generate an optimal location, the generated optimal location is given to the user. So that user can only know his/ her own preferred or current location but not others. For the first time if the optimal location is not generated, once again PPFRVP is going to generate optimal point so that it will be in minimum distance to all other users.

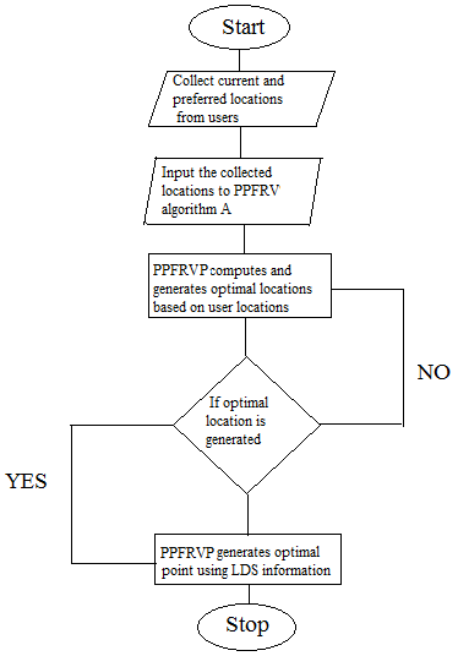

Fig.3. Flow Chart for Discovering the Optimal Meeting Location for the Protection of Privacy of Mobile Device Users.

IV. RESULTS AND DISCUSSION

In this chapter, We show the evaluation of proposed PPFRVP protocols by using graph the results of controlled experiments and conducted user studies using prototype implementation of protocols on mobile devices.

A. DISTANCE COMPUTATIONS

As we have discussed, the FRVP L_{fair} is nothing but the preference of location that minimizes the maximum distance of any other preference of location and L_{fair}. Our algorithm minimize with respect to the square of the distances, this is because distance square can be easily computed using homomorphic encryptions than distances which are simple. The squaring function will preserve order and the problem which is of finding the arguments which minimizes the maximum distance that is equivalent to finding the argument which minimizes the maximum squared distance.

1) *BGN-Distance*: First let us consider the BGN encryption sceme as a distance computation algorithm. Thisprotocol needs only one time communication with each user and LDS. It utilizes both additive and multiplicative homomorphic properties of BGN. This BGN scheme works in the following fashion.

$E_i(a) = < a_{i1}|. . . | a_{i6} > = < E(x_i) | E(T- 2x_i) | E | E(T-2y_i) | E(y_i) | E(1) >$

$Ei(b) =< b_{i1}| . . . | b_{i6} > = < E(1) | E(x_{i_2}) | E(y_i) | E(1) | E(y_{i_2}) >$

Where, E (.) is termed as the encryption which is using the BGN scheme with K_P^{Mv}which is nothing but fresh session key. Li = (xi,yi) which is called as desired randez-vous user location u_i and Tisthe modulus of domain of plaintext.

2) *Paillier- Elgamal- Distance*: An another schene for computation of distance is based on both ElGamal andPaillier encryptions, Including Elgamal multiplicative homoorphic property, we depend on the two features of paillier encryption as follows:

$$E(m_1) \cdot E(m_2) = E(m_1 + m_2 \bmod n), \forall m_i \in Zn \quad (1)$$

$$E(m_1)^r = E(r \cdot m_1 \bmod n), \forall r \in Z^* n \quad (2)$$

Which indicates that

$$E(r \cdot m1)^{r-1} = E(r^{-1} \cdot r \cdot m_1 \bmod n) = E(m_1 \bmod n) \quad (3)$$

Here, r^{-1} is called as multiplicative inverse of r mod n. As neither ElGamal or Paillier has both additive and multiplictive properties, resultant

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

algotithm need of extra step to compute the pairwise squared distances i.e. d_{ij}^2[13].

B. MEASUREMENT of PERFORMANCE and IMPLEMENTATIONS

Implementation of client application on Nokia N810 mobile devices (256 MB RAM, ARM 400 MHz CPU, Maemo OS, Linux) and the implementation of LDS is running on a standard Linux PC (3 GB RAM, 2 GHz CPU, Linux). Our applications are implemented on Qt programming framework.

We show in fig. 4(a), 4(b) and 4(c) that the time of computation is increased by increasing number of users. However, the ElGamal-paillier based method is more effective and efficient across all other computations, Only 4 seconds are required to execute a protocol with participants of 10 numbers. The 2 BGN algorithms are less effective and efficient required 9 seconds of time compared to ElGamal-paillier algorithm. The reason for this is because of bilinear mapping operations of CPU of the BGN cryptosystem.

Fig. 4(d), 4(e) show different times of computation on Nokia N810 mobile device. We have seen that BGN based algorithm is most efficient in distance computations, which requires 0.3 seconds, independent of number of users. This is because the clients can send only once its own encrypted vectors to allow LDS to compute distances of all pairs, which is opposite to ElGamal-Paillier based algorithm requires that user need to encrypt and decrypt values number of times based on number of users. An another protocol, require 4 seconds for 10 participants. In the following phases, result is not better because the BGN-based protocol use intensively the bilinear mapping operations. If we see the overall performance of ElGamal-Paillier is better.

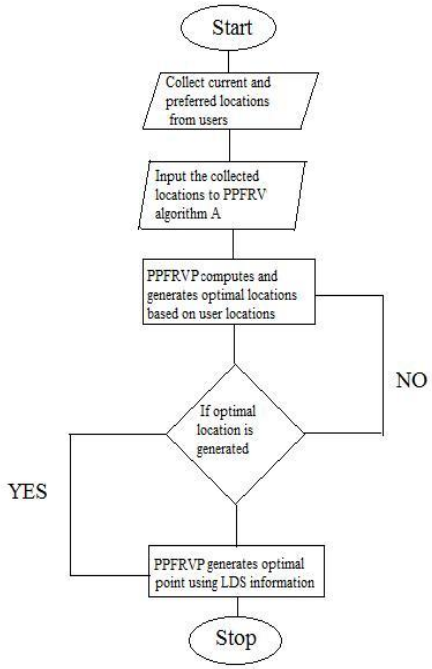

Fig. 4. Discuss the Performance measurements of (a) LDS distance computations. (b) LDS maximum computations. (c) LDS minimum computations. (d) Client distance computations. (e) Client max/argmin computations. (d) Total client and LDS run times.

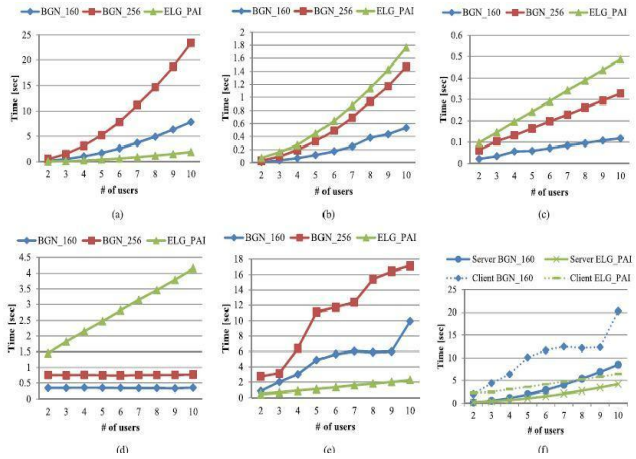

Fig.4.Performance measurements. (a) LDS distance computations. (b) LDS maximum computations. (c) LDS minimum computations. (d) Client distance computations. (e) Client max/argmin computations. (d) Total client and LDS run times.

V. CONCLUSION AND FUTURE WORK

We proposed the preservation of privacy of mobile users by collecting the preferred locations of the users by finding the optimal location in FRVP (i.e. Fair Rendez-Vous problem). Solution of this work relies on the homomorphism features of cryptosystems which are well known. We have implemented algorithm and performance is evaluated on mobile devices. We have showed that the performance evaluated in real time is accepted widely because of effective preservation of privacy. At last, we proved that the privacy preservation is the important point in while using the mobile device applications.

REFERENCES

[1] E. Valavanis, C. Ververidis, M. Vazirgianis, G. C. Polyzos, and K. Norvag, "MobiShare: Sharing context-dependent data & services from mobile sources," in

[2] *Proc. IEEE/WIC Int. Conf. WI* pp. 263–270, (Oct. 2003)

[3] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. 7th Int. Conf. Pervasive Computing*, pp. 390–397, (2009)

[4] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services," in *Proc. 15th Int. Conf. Financial*, pp. 31–46, (2011)

[5] J. Freudiger, M. Jadliwala, J.-P. Hubaux, V. Niemi, P. Ginzboorg, and I. Aad, "Privacy of community pseudonyms in wireless peer-to-peer networks," *MobileNetw. Appl.*, vol. 18, no. 3, pp. 413–428, (2012)

[6] J. Krumm, "A survey of computational location privacy," *PersonalUbiquitous Comput.*, vol. 13, no. 6, pp. 391–399, (2009).

[7] V. Vazirani, *Approximation Algorithms*. New York, NY, USA: Springer-Verlag, (2001).

[8] I. Bilogrevic, M. Jadliwala, K. Kalkan, J. Hubaux, and I. Aad, "Privacy in mobile computing for location-sharing-based services," in *Proc. 11th Int. Conf. PETS*, 2011, pp. 77–96.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACMSIGMOD*, , pp. 121–132, (2008)

[10] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," *IEEETrans. Mobile Comput.*, vol. 9, no. 6, pp. 810–823, (Jun. 2010)

[11] C.-H. O. Chen *et al.*, "GAnGS: Gather, authenticate 'n group securely," in *Proc. 14th ACM Int. Conf. Mobile Computing Networking*, pp. 92–103, (2008)

[12] Y.-H. Lin *et al.*, "SPATE: Small-group PKI-less authenticated trust establishment," in *Proc. 7th Int. Conf. MobiSys*, pp. 1–14, (2009)

[13] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, (1978)

[14] O. Goldreich, *Foundations of Cryptography:Basic Applications*. Cambridge, U.K.: Cambridge Univ. Press, (2004).

[15] K. B. Frikken and M. J. Atallah, "Privacy preserving route planning," in *Proc. ACM WPES*, 2004, pp. 8–15.

[16] S.-D. Li and Y.-Q. Dai, "Secure two-party computational geometry," *J. Comput. Sci. Technol.*, vol. 20, no. 2, pp. 258–263, (2005).

[17] A. Solanas and A. Martínez-Ballesté, "Privacy protection in location based services through a public-key privacy homomorphism," in *Proc.4th European Conf.Public Key Infrastructure, Theory and Practice*, pp. 362–368, (2007)

[18] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, Lester and Pierre: Three protocols for location privacy," in *Proc. 7th Int. Conf. PrivacyEnhancingTechnologies*, pp. 62–76, (2007)

[19] S. Jaiswal and A. Nandi, "Trust no one: A decentralized matching service".

[20] Igor Bilogrevic, *Member, IEEE*, Murtuza Jadliwala, *Member, IEEE*, Vishal Joneja, Kübra Kalkan, Jean-Pierre Hubaux, *Fellow, IEEE*, and Imad Aad, "Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices", IEEE transactions on information forensics and security, vol. 9, no. 7, (July 2014)

[21] *Facebook Statistics* [Online]. Available:http://www.facebook.com/press/info.php?statistics (Nov. 2011).

[22] *Facebook Deals* [Online]. Available: http://www.facebook.com/deals/ (Nov. 2011)

[23] *Let's Meet There* [Online]. Available:http://www.letsmeetthere.net/ (2011).

[24] *Please Rob Me* [Online]. Available:http://pleaserobme.com/[11] (Nov. 2011)

[25] *Microsoft Survey on LBS* [Online]. Available: http://go.microsoft.com/?linkid=9758039, (2011).

[26] *Orange Taxi Sharing App* [Online]. Available: http://event.orange.com/default/EN/all/ mondial (Nov. 2011).

[27] *UTM Coordinate System* [Online]. Available:https://www.education.psu.edu/natureofgeoinfo/c2_p21.html(Nov. 2011)

Student Profile:

Parameswari.T,I am received B.Tech from School of Engineering And
Technology, Sri Padmavathi Mahila University,Tirupati. I am pursuing
PG in C.S.E from MLEC,JNTU
Kakinada,Kanumalla,SingarayaKonda,Prakasam(D.t),AP,India.
parameswarituraka@gmail.com

Guide Details:

T.SREEKANTH
B.Tech., M.Tech.
ASST.PROFESSOR
MLECJNTU
Kakinada,Kanumalla,SingarayaKonda,Prakasam(D.t),AP,India.
sreekanth.thullibilli@gmail.com