International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.07,Issue.06,
July-2015,
Pages:0894-0897

www.ijatir.org

Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices

RAMAKRISHNA KOLIKIPOGU[1], K. SWETHA[2]

[1]Dept of IT, Sridevi Women's Engineering College, Hyderabad, TS, India, E-mail: krkrishna.csit@gmail.com.
[2]Dept of IT, Sridevi Women's Engineering College, Hyderabad, TS, India, E-mail: kora.swetha@gmal.com.

Abstract: Nowadays, it is very facile for a person to learn his/her location with the avail of a Ecumenical Situating System (GPS) enabled contrivance. A location-predicated accommodation(LBS) is an incipient and developing technology for mobile users. When this location is provided to LBS via querying, it is possible to learn location dependent information, such as locations of friends or places, weather or traffic conditions around the location. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kenned as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. In this paper, we determine the privacy-preserving optimal meeting-location quandary and the obligatory privacy requisites that have got to be satisfied by whatever algorithm that solves ye POML problem.

Keywords: Location-Predicated Accommodation, Points Of Interest (POIs), Privacy-Preserving Optimal Meeting-Location (POML).

I. INTRODUCTION

The rapid proliferation of Smartphone technology in urbanized communities has modified mobile users to use circumstance ware accommodations on their contrivances. Accommodation providers capitalize on this dynamical and ever- producing technology landscape by suggesting innovatory context-dependent accommodations as mobile subscribers. Location-predicated Accommodations (LBS) [3], for example, are utilized by billions of mobile subscribers all twenty-four hour period to find location-concrete data. Two popular features of location-predicated accommodations are location check-ins plus location share-out. By checking into a position, users can allocate their current location on family plus friends or receive location-cover accommodations from third-party providers. The obtained accommodation does not depend on the locations of early users. The early types of location-predicated accommodations, which trust on share-out of positions (or position predilections) through a group of utilizers in order to find more or less accommodation for the whole group, are withal propagating. According to a recent study, location sharing accommodations are utilized by virtually 20% of totally mobile phone utilizers. One outstanding example from such an accommodation is the taxi-sharing application, offered by an ecumenical telecom operator, where Smartphone users can apportion a taxi with other users at a congruous location by exposing their difference and terminus locations.

Likewise, some other democratic accommodation modifies a group of utilizers to determine the majority geographically convenient position to meet. Secrecy of a utilizer position or position predilections, with deference to other users and the third-party accommodation supplier, is a vital concern in this location sharing predicated applications. For instance, such information can be habituated to deanonymize users and their availabilities, to track their predilections or to identify their gregarious networks. Because example, in ye taxi- share-out application, a curious third-party adjustment provider could facilely deduce home/work position couples of users who conventionally use their accommodation. Without efficacious auspice, still sparse position data has made up shown to provide reliable data about a utilizers private area, which could hold astringent consequences on the users' gregarious, financial and private life. Even accommodation suppliers who lawfully track utilizers position data in prescribe to amend the offered accommodation can inadvertently harm users' privacy, if the accumulated information is leaked out in an unauthorized fashion or malapropos shared on corporate partners.

Recent utilizer studies [4],[5],[7] show that end-users are prodigiously sensitive about sharing their location information. Our study on 35 participants, including students and non-scientific staff, showed that proximately 88% of users were not comfortable sharing their location information. Thus, the disclosure of private location in any Location-Sharing-Predicated Accommodation (LSBS) is an major business and must live addressed. In this Proposal, we deal ye secrecy effect in LSBSs by fixating on a concrete quandary called the Fair Rendez-Vous Point (FRVP) quandary. Given a set of utilizer location predilections, the FRVP quandary is to find out a location amongst the suggested ones such that the upper limit distance amongst this location plus totally other users' locations is minimized, i.e. it is fair to totally utilizers. Our goal is to supply practical privacy-preserving techniques to clear the FRVP problem , such that neither a third-party, nor taking part utilizers, can memorize other users' locations; entering utilizers only learn the optimum location.

II. RELATED WORK

The mobile contrivances we utilize in everyday life is incremented due to the rapid development of wireless communication technology and mobile computing, they are habituated to amass the information and accommodation providers by complementing or superseding fine-tuned location hosts connected to the wire line network. Such mobile resources can be highly consequential for other moving users, engendering paramount opportunities for many fascinating and novel applications. The mobile architecture provides the infrastructure for ubiquitous mobile access and it withal provides the mechanism for publishing, discovering and accessing heterogeneous mobile resources in an immensely colossal area taking into account for both resources and requestors. Thus the overall approach is considered to be data centric and accommodation oriented, implicatively insinuating that contrivances are treated as engenderers or requestors as information accommodation providers. Utilizer location data is benefit to many applications, but they raise the privacy concerns.

Anonymization[14] can bulwark the privacy quandary. By considering location data for utilizer who live and work in different regions can be re-identified facilely. Thus the re-identification is the best process for the deduction of home and work location. The anonymity is preserved by offering the location traces before they disclose. One more technique is computational location privacy, betokening computational-predicated privacy mechanism that treats the location data as geometric information. It mainly deals with the study of people's posture about location privacy, computational treats on leaked location data, and provides the counter measures for mitigating these treats. In modern mobile networks the users increasingly share their location with the third party users in reciprocation for location predicated accommodation. Users obtain accommodations customized to their location, yet such communications leak location information about the users. By performing the authentic mobility traces and quantifying dynamics of users privacy for fends the location predicated accommodation.

III. PROPOSED WORK

In this section, we determine the privacy-preserving optimal meeting-location problem plus the mandatory privacy requirements that experience to be met by whatever algorithm that solves the POML problem.

A. Privacy-Preserving Optimal Meeting-Location Problem

In this work, we consider the quandary of finding, in an privacy-preserving direction, ye optimal gathering location between various players, this that (i) for each one of the users acquires to ken alone the final optimum location plus (ii) no utilizer or third party server kens any other private location information about any user demanded in the computations. We refer to an algorithm that solves such quandary as privacy-preserving optimal meeting-location algorithm. In universal, whatever POML algorithm A ought work as comes. Given a fixed of N utilizers U, where for each one utilizer u_i, $i \in \{1,...,N\}$, gives a private favored location L_i, and a transmutation role f, the POML algorithm accepts $f(L_i)$, $\forall i \in \{1,...,N\}$, as inputs plus computes ye location role $f(L_{opt})$ as output, where L_{opt} is ye optimum location as calculated by an optimization role g, afforded the private inputs $f(L_1),...,f(L_N)$. Furthermore, the inputs to the algorithm and the outputs it makes should satiate ye two privacy necessities reported earliest. Fig.1 demonstrates a operational diagram of a POML protocol, whereas the POML algorithm A is performed by an LDS. Officially, a POML algorithm A functions as comes:

Input: a transmutation f of secret locations L_i

$$f(L_1)||f(L_2)|| \ldots ||f(L_N) \qquad \textbf{(1)}$$

Whereas f is a one-way public role (predicated on private key) such that it is difficult (successfulness with only a negligible chance) to decide ye input L_i minus kenning the private key, by just watching $f(L_i)$.

Output: an output $f(L_{opt}) = g(f(L_1),...,f(L_N))$, whereas g is an optimization role and $L_{opt} = (x_l, y_l) \in N_2$ is the optimal gathering location that has been picked for this special set of users, such that it is hard for the LDS to decide L_{opt} by just watching $f(L_{opt})$. Given $f(L_{opt})$, each user is able to work out $L_{opt} = f^{-1}(f(L_{opt}))$ using his local data.

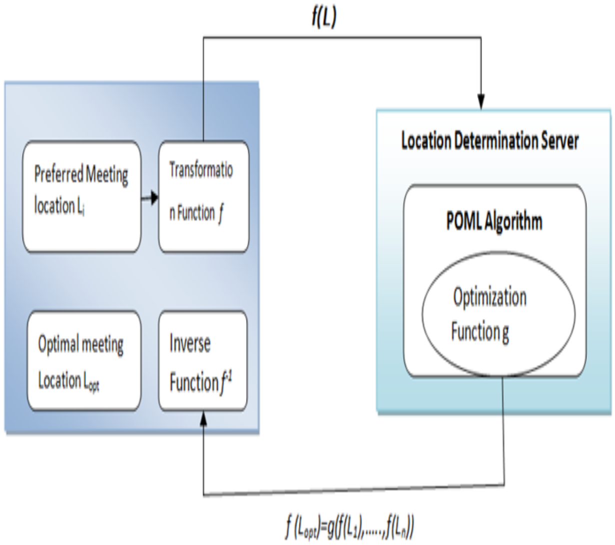
f(L)
Preferred Meeting location L_i
Transformation Function f
Optimal meeting Location L_opt
Inverse Function f^-1
Location Determination Server
POML Algorithm
Optimization Function g
f(L_opt)=g(f(L_1),.....,f(L_n))

Fig.1. Operational diagram of the POML protocol, whereas the POML algorithm is accomplished by an LDS.

The optimization work g can be determined in various ways, depending on ye predilections from the utilizers, their employers or policies. For example, utilizers may choose to meet in locations that are close to their offices, plus their employers may choose a place that is most close to their utilizers.

B. Privacy Requirements and Definitions

The generic POML protocol represented in Fig.1 necessitates various procedures, some of which are performed on the utilizer convenience plus some on a third-party LDS.

Moreover, the PS is optionally required by the users in order to obtain the location coordinates of POIs in a committed area. In dictate to assure that private data about utilizers is not leaked out to other utilizers or third-parties throughout the performance of ye POML algorithm, we need to formally define requisites that any such algorithm has to satiate. Afterwards, we will evaluate the proposed POML algorithms predicated on these privacy definitions. Informally, the privacy requisites can be verbalized as comes. Afterward the performance of the POML algorithm, whatever utilizer u_i should non equal able to infer (i) the favored location L_j of any other utilizer $u_j \neq u_i$ nor (ii) the relative distances d_{ij} between whatever 2 utilizers $u_i \neq u_j$. Similarly, whatever LDS (plus PS) should non be capable to understand (iii) the favored location Li of any utilizer ui, (iv) the relative outdistance d_{ij} among any 2 utilizers $u_i \neq u_j$ nor (v) the last meeting position L_{opt}. this privacy requirements can be grouped in 2 elements, called as utilizer-privacy and server-privacy, defined as follows .

C. User-Privacy

The utilizer-privacy of any POML algorithm A evaluates the probabilistic reward that an assailant a (a utilizer entering in the POML protocol or an outside user) benefits toward seeing the favored location L_j of at to the lowest degree 1 other utilizer $j \in \{1,...,N\}$, exclude the concluding optimal meeting place L_{opt}, after all utilizers have entered in the performance of POML protocol. Pellucidly, an external utilizer performs not learn about any favored locations as it performs not receive the yield of the algorithm. Hence, we just conceive the non-nugatory event of utilizer taking part in the POML protocol as aggressors, i.e., ua where $a \in \{1,...,N\}$. We express the utilizer-privacy in terms of 3 adversary rewards. 1st, we quantify the specifiable advantage, which is the probabilistic reward of u_a in right conjecturing the preferred location Li of any utilizer $u_i \neq u_a$. We denote it as Adv^{IDT}_a (A). Second, we measure the space linkability reward, which is the probabilistic reward of ua in right supposing whether the space dij among any two utilizers $u_i \neq u_j$, is more preponderant than a given parameters, without obligatorily kenning any users' preferred locations L_i, L_j . We denote this advantage as Adv^{d-LNK}_a. Conclusively, we measure the coordinate-link ability reward, which is the probabilistic reward of u_a in correctly supposing whether a afforded coordinate x_i (or y_i) of a utilizer u_i is more preponderant than the corresponding coordinate(s) of another utilizer $u_j \neq u_i$, i.e., x_j (or y_j), minus indispensably kenning any users' favored locations L_i, L_j . We announce this reward as Adv^{c-LNK}_a .The following observation follows from the over definitions.

Observation 1: If an adversary has an recognizable reward over any 2 distinct utilizers $u_i \neq u_j$, this implicatively insinuates it has distance- and coordinate-link ability advantages over those two users as well. However, the inverse is not indispensably true. We semantically determine the identifiability plus linkability rewards by using a challenge-replication methodology, which has been wide utilized to demonstrate the surety of cryptographic protocols. We now describe such a challenge-replication game for the identifiability advantage Adv^{IDT}_a (A) of any adversary u_a in a POML algorithm A.

- **Initialization:** Challenger privately collects $L = \{L_i\}^N_{i=1}$, where $Li = (x_i, y_i)$ is the preferred meeting location of user u_i, and $f(Li)$, $\forall i \in \{1,...,N\}$.
- **POML algorithm:** Challenger executes the POML algorithm A with the N users and computes $f(L_{opt}) = g(f(L1),...,f(LN))$. It then sends $f(L_{opt})$ to each user u_i, $\forall i \in \{1,...,N\}$.
- Challenger randomly chooses a user u_a, $a \in \{1,...,N\}$, as the adversary.
- u_a chooses $u_j \neq u_a$ and sends j to the challenger.
- Challenge: Challenger chooses a random $k \in \{1,...,N\}$, $k \neq a$ and sends L_k to the adversary. The challenge is to correctly guess whether $L_k = L_j$.
- The adversary sends $L*_j$ to the challenger. If the adversary thinks that L_k is the preferred meeting location of user u_j , i.e., if $L_k = L_j$ then the adversary sets $L*_j = 1$. If the adversary thinks that L_k is not the preferred meeting location of user u_j , then he sets $L^*_j = 0$.

D. Server-Privacy

The server-privacy of any POML algorithm A measures the probabilistic advantage that the LDS gains in learning the preferred meeting locations L_i of any utilizer u_i, $i \in \{1,...,N\}$. As in the case of utilizer-privacy, we express the server-privacy by denotes of three advantages. First, we quantify the probabilistic advantage of an LDS in correctly conjecturing the preferred location L_i of any utilizer u_i, called identifiability advantage and denoted as $Adv^{IDT}_{LDS}(A)$. Second, we quantify the probabilistic advantage of an LDS in correctly conjecturing whether the distance d_{ij} between any two users $u_i = u_j$ is more preponderant than a given parameter s, without compulsorily kenning any users' preferred locations L_i, L_j . We call this the distance-linkability advantage and we denote it as Adv^{d-LNK}_{LDS} (A). Third, we quantify the probabilistic advantage in correctly conjecturing whether a given coordinate x_i (or y_i) is more preponderant than the same coordinate of another utilizer j= i, i.e., x_j (or y_j), without compulsorily kenning any users' preferred locations L_i, L_j . We call this the coordinate link ability advantage and we denote it as Adv^{c-LNK}_{LDS} (A). The server identifiability and link ability advantages are defined in a homogeneous fashion as the utilizer advantages, and are presented in Appendix A.

IV. EXPERIMENTAL RESULT

To the best of our cognizance, this is the first function to address the optimum meeting-location problem with secrecy assures as shown in Fig.2. Future, we first give recent functions that address, minus bulwarking secrecy, strategies to find out the optimal assembling location. Then, we talk about contributions in insure multiparty computation on point-distance calculations. Note that we guided the experimentations in groups of 4-5 participants, hence one utilizer out of 4-5 was the one who apperceived his own location as making up the optimal location.

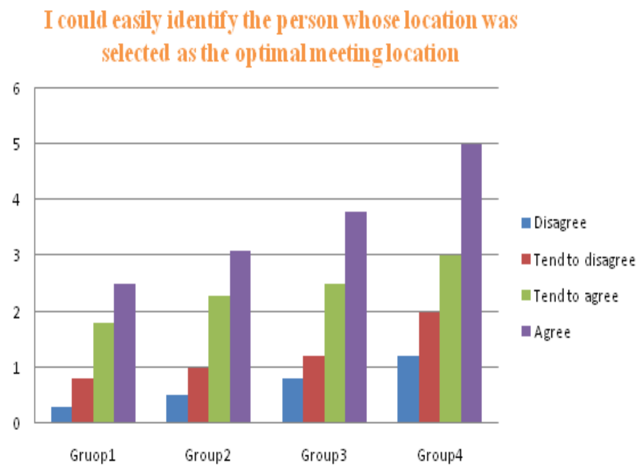

Fig.2.Resuls.

V. CONCLUSION

Activity management applications are frequently utilized by people in order to facilitate the orchestrating of their circadian obligations. Privately establishing mundane time availabilities is a consequential job for all participants, plus substantial research exertion has already been committed to such a dispute. In this employment, we addressed the complementary problem of expeditiously and privately computing the optimal meeting location, and presented two privacy-preserving protocols that solve such quandary. To the best of our cognizance, this is the first work that addresses the privacy concerns in optimal meeting-location tenaciousness. By designates of analytical evaluation and practical implementation on authentic mobile contrivances, we expressed that our systems efficiently compute the optimum meeting location plus do not expose any private data. Furthermore, our user-study showed that people are concerned about sharing personal location predilections with untrusted parties, which increases the pertinence of our research efforts and reinforces the desideratum for further exploration.

VI. REFERENCES

[1] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM Transactions on Computer Systems, 1(3):239–248, 1983.

[2] Paramvir Bahl and Venkata N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In Proceedings of IEEE INFOCOM ’00, pages 775–784, Tel Aviv, Israel, March 2000.

[3] J. Bailey. Internet price discrimination: Self-regulation, public policy, and global electronic commerce. http://www.tprc. org/abstracts98/bailey.pdf.

[4] A. R. Beresford and F. Stajano. Location privacy in pervasivecomputing. IEEE Pervasive Computing, 1:46–55, 2003.

[5] Dan Boneh. The decision Diffie-Hellman problem. In ANTSIII, volume 1423 of Lecture Notes in Computer Science, pages 48–63, 1998.

[6] P. Castro, P. Chiu, T. Kremenek, and R. Muntz. A probabilistic room location service for wireless networked environments. In Proceedings of Ubicomp, 2001.

[7] Dan Gusfield and Robert W. Irving. The Stable Marriage Problem: Structure and Algorithms. MIT Press, Cambridge, MA, USA, 1989. ISBN 0-262-07118-5.

[8] Carmit Hazay and Yehuda Lindell. Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. In Theory of Cryptography Conference, 2008.

[9] Yan Huang. Fast Secure Computation Framework. http://www.MightBeEvil.org/framework/, 2011.

[10] L. Sweeney, “k-Anonymity: A model for protecting privacy,” Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002

[11] A. Beresford and F. Stajano, “Location privacy in pervasive com-puting,”IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar.2003.

[12] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” J. ACM, vol. 45, no. 6, pp. 965–981, 1998

[13] L. Girod and D. Estrin. Robust range estimation using acoustic and multimodal sensing. In IEEE/RSI Int. Conf. on Intelligent Robots and Systems (IROS), 2001.

[14] S. Goldwasser and M. Bellare. Lecture notes on cryptography. Summer Course Lecture Notes at MIT, 1999.

[15] Andreas Gorlach, Andreas Heinemann, and Wesley W. Terpstra.Survey on location privacy in pervasive computing. In Workshop on Security and Privacy in Pervasive Computing, April 2004.

[16] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of The First International Conference on Mobile Systems, Applications, and Services (MobiSys), June 2003.