Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices

Samta M. jain
Department of Computer Technology
Rajiv Gandhi College Of Engineering Research & Technology
Chandrapur.MH(India)
e-mail:Samtajain7123@gmail.com

Abstract- LBS is the ability to protect connection between users identity, servers , database thereby preventing attacker from easily linking of users of LBS to certain location. For todays urban population, smart phones has become most important gadget for maintaining the daily activities. Users uses such type of application to plan their daily routine. These Application often relay on current location of individual users or a group of users to provide the desired services. By means of such applications users population reveal their current location to the third party service providers. Thus knowingly or unknowingly they loss their privacy. Users who cautions about their security, do not necessarily want to reveal their current location to service provider or to untrusted users. Thus in this paper we proposes privacy-preserving algorithm for determining an optimal meeting location for a group of users. This is to provide practical privacy –preserving techniques to solve this problem, such that neither an untrusted user, nor participating users, can learn other users locations, legitmate users only learn optimal locations.

Keywords: *Location Privacy, GSM ,Security*

*****

I. INTRODUCTION

Location-based Services (LBS) are employed by several mobile subscribers to get location specific information [1].Two popular features of location-based services are location check-ins and sharing-location. users can share their current location by checking the location with family and friends or access location-specific services from third-party providers. Location privacy is the ability to prevent others parties from learning ones current or past location Generally, Location Based Service (LBS) gives an information service about the physical location of a user [9]. Privacy of a user's location or location preferences, with relevance and therefore third-party service provider, may be an essential concern in such location-sharing-based applications. For instance, such information can be used to de-anonymize users and their availabilities [3], to track their preferences [4] or to identify their social networks [5].

Without effective protection ,if the collected data is leaked in an unauthorized fashion or improperly shared with corporate partners,which could have severe consequences on the on the users social , financial and private life [6], [7]. Thus, the disclosure of private location in any Location-Sharing-Based Service (LSBS) is a major concern and must be addressed.

In this work, we address the privacy issue in LSBSs by focusing on a specific problem called the *Fair Rendez-VousPoint (FRVP)* problem,such that :

(i) The Rendez-Vous point is *fair* with respect to the given input locations

(ii)Each user learns only the final Rendez-Vous location and

(iii)No participating user or third-party server learns private location preference of any other user involved in the computation.

The algorithm termed as *Privacy-Preserving Fair Rendez-Vous Point (PPFRVP)* algoritm.

II. SYSTEM ARCHITECTURE

We consider a system composed of two main entities: (i) aset of users1 (or mobile devices) U = {$u1, . . . , uN$ } and (ii) athird-party service provider, called *Location Determination Server (LDS)*, which is responsible for privately computing the fair rendez-vous location or point from a set of userpreferred rendez-vous locations. Each user's mobile device is able to communicate with the LDS by means of some fixed infrastructure-based Internet connection. Each user *ui* has the means to determine the coordinates $Li = (xi , yi) \in$ N2 of his preferred rendez-vous location. We consider a two-dimensional coordinate system, but the proposed schemes are general enough and can be easily extended to other higher dimensional coordinate systems [14]. Users can either use their current position as their preferred rendez-vous location or they can specify some other preferred location (e.g., a point-of-interest such as a known restaurant) away from their current position. Users determine their current position (or positions of known points-of-interest) by using a positioning service, such as Global Positioning System or GPS. We assume that the positioning service is fairly accurate. GPS, for example, has an average positioning error between 3 and 7.8 meters. We would like the readers to note that the goal of the positioning service is only to enable users to determine or select their preferred location, and that it should not be confused with the LDS. Users can continue to use the service of the LDS for privately computing the fair rendezvous location without using the positioning service, say by manually estimating their preferred rendez-vous location. A positioning service, if used, can continuously track users based on the positioning requests or it can behave maliciously and provide incorrect position information (or position information with large errors) to the users. In this work, we do not consider these adversarial scenarios involving the positioning service as these are orthogonal to the privacy preserving FRVP problem. In order to limit the information that the positioning service learns about the users' location requests, a private information retrieval technique [15] can be used. Moreover, a secure positioning system [16] can be used to overcome the problem of cheating within the positioning service.

We define the set of the preferred rendez-vous locations of all users as L = {*Li* }*Ni*=1. For the sake of simplicity, we consider line-of-sight Euclidean distances between preferred rendez-vous locations. Even though the actual real-world distance (road, railway, boat, etc.) between two locations is at least as large as their Euclidean distance, the proportion between distances in the real world is assumed to be correlated with the respective Euclidean distances. publicly known and users encrypt their input to the FRVP algorithm using this key; the encrypted input can be decrypted by the LDS using its private key *K LDs* . This ensures message confidentiality and integrity. For simplicity, we do not explicitly show the cryptographic operations involving LDS's public/private key.

III. EXISTING SYSTEM

The rapid proliferation of smart phone technology in urban communities has enabled mobile users to utilize context aware services on their devices. Service providers take advantage of this dynamic and ever-growing technology landscape by proposing innovative context-dependent services for mobile subscribers. Location-based Services (LBS), for example, are used by millions of mobile subscribers every day to obtain location-specific information .Two popular features of location-based services are *location check-ins* and *location sharing*. By checking into a location, users can share their current location with family and friends or obtain location-specific services from third-party providers ,The obtained service does not depend on the locations of other users. The other type of location-based services, which rely on sharing of locations (or location preferences) by a group of users in order to obtain some service for the whole group, are also becoming popular. According to a recent study , location sharing services are used by almost 20% of all mobile phone users. One prominent example of such a service is the taxi-sharing application, offered by a global telecom operator , where smart phone users can share a taxi with other users at a suitable location by revealing their departure and destination locations. Similarly, another popular service enables a group of users to find the most geographically convenient place to meet.

Problems on existing system:

1.Privacy of a user's location or location preferences, with respect to other users and the third-party service provider, is a critical concern in such location-sharing-based applications. For instance, such information can be used to de-anonymize users and their availabilities, to track their preferences or to identify their social networks. For example, in the taxi-sharing application, a curious third-party service provider could easily deduce home/work location pairs of users who regularly use their service.

2. Without effective protection, evens parse location information has been shown to provide reliable information about a users' private sphere, which could have severe consequences on the users' social, financial and private life. Even service providers who legitimately track users' location information in order to improve the offered service can inadvertently harm users' privacy, if the collected data is leaked in an unauthorized fashion or improperly shared with corporate partners.

IV. PROPOSED SYSTEM

We then propose two algorithms for solving the above formulation of the FRVP problem in a privacy-preserving fashion, where each user participates by providing only a single location preference to the FRVP solver or the service provider.

In this significantly extended version of our earlier conference paper, we evaluate the security of our proposal under various passive and active adversarial scenarios, including collusion. We also provide an accurate and detailed analysis of the privacy properties of our proposal and show that our algorithms do not provide any probabilistic advantage to a passive adversary in correctly guessing the preferred location of any participant. In addition to the theoretical analysis, we also evaluate the practical efficiency and performance of the proposed algorithms by means of a prototype implementation on a test bed of Nokia mobile devices. We also address the multi-preference case, where each user may have multiple prioritized location preferences. We highlight the main differences, in terms of performance, with the single preference case, and also present initial experimental results for the multi-preference implementation. Finally, by means of a targeted user study, we provide insight into the usability of our proposed solutions.

Advantages of proposed system:

We address the privacy issue in LSBSs by focusing on a specific problem called the Fair Rendezvous Point (FRVP) problem. Given a set of user location preferences, the FRVP problem is to determine a location among the proposed ones such that the maximum distance between this location and all other users' locations is minimized, i.e. it is fair to all users.

V. IMPLEMENTATION

A. Modules:

1. User Privacy
2. Server Privacy
3. PPFRVP protocol
4. Privacy Under Multiple Dependent Executions

B. Module description

User Privacy:

The user-privacy of any PPFRVP algorithm A measures the probabilistic advantage that an adversary a gains towards learning the preferred location of at least one other user ,except the final fair rendez-vous location, after all users have participated in the execution of the PPFRVP protocol. An adversary in this case is a user participating in A. We express user-privacy as three different probabilistic advantages.

1.We measure the probabilistic advantage of an adversary *ua* in correctly guessing the preferred location *Li* of any user *ui* _= *ua*. This is referred to as the identifiability *advantage.*

2.The second measure of user-privacy is the *distance linkability advantage*, which is the probabilistic advantage of an adversary *ua* in correctly guessing whether the distance*d i, j* between any two participating users *ui* _= *u j* , is greater than a given parameter *s*, without learning any users' preferred locations *Li* , *L j.*

3.The coordinate-likability advantage, denoted as Advc−LNKa , is the probabilistic advantage of an adversary ua in correctly guessing whether a given coordinate xi (or yi)of a user ui is greater than the corresponding coordinate(s)of another user u j _= ui without learning the users' preferred locations Li , L j .

Server Privacy:

For the third-party (LDS) adversary, the game definitions are similar to those defined for an user adversary, except that the LDS does not receive L f air in the Step 2 of the game. Then, the server-privacy of a PPFRVP algorithm A can then be defined as follows. Definition 3: An execution of the PPFRVP algorithm A is server-private if the identifiability advantage DTLDS(A), the distance-linkability advantage Advd−LNKLDS and the coordinate linkability advantage Advc−LNKLDS of an LDS are negligible. In practice, users will execute the PPFRVP protocol multiple times with either similar or completely different sets of participating users, and with the same or a different location preference in each execution instant. Thus, although it is critical to measure the privacy leakage of the PPFRVP algorithm in a single execution, it is also important to study the leakage that may occur over multiple correlated executions, which in turn depends on the intermediate and final output of the PPFRVP algorithm. We discuss the privacy leakage of the proposed algorithms over multiple executions in Section VI-D.

PPFRVP protocol:

The PPFRVP protocol (shown in Fig. 4) has three main modules:
(A) the distance computation module,
(B) the MAX module and

1) Distance Computation: The distance computation module uses either the BGN-distance or the Paillier-ElGamal distance protocols. We note that modules (B) and (C) use the same encryption scheme as the one used in module (A). In other words, (*E).It* refers to encryption using either the BGN or the Paillier encryption scheme.

2) MAX Computation: In Step B.1, the LDS needs to hide the values within the encrypted elements (i.e., the pair wise distances computed earlier) before sending them to the users.
This is done in order to

(i) ensure privacy of real pair wise distances,
(ii) be resilient in case of collusion among users and
(iii) preserve the internal order (the inequalities) among the pair wise distance from each user to all other users.

Privacy Under Multiple Dependent Executions:

As defined earlier, in a dependent execution of the PPFRVP protocol, all the involved parties possess information from the previous executions, in addition to the current input, output and intermediate data. It is clear that, due to the oblivious or blind nature of the computations, the privacy guarantees of the proposed PPFRVP protocols with respect to the LDS independent executions remains the same as that for independent executions. Furthermore, dependent executions in which the information across executions is completely uncorrelated (e.g., different set of users in each execution or different and unrelated preferences in each execution) reduce to independent execution. We analyze two different scenarios of dependent executions involving differential information .First, we consider the case of dependent executions with different subsets of participants. We assume that, in each sequential execution, the set of users or participants is reduced by exactly one (the adversary participant remains until the end), and that the retained participants preferences remain the same as the previous execution(s). The following information is implicitly passed across executions in this scenario:

(i) participant set,
(ii) optimal fair location *L f air* ,
(iii) permuted and randomly scaled pair wise distances from

the participant to every other participant, and (iv) scaled (but order preserving) maximum distance from every participant to every other participant.

VI. CONCLUSION

In this work, we addressed the privacy issue in the Fair Rendez-Vous Problem (FRVP). Our solutions are based on the homomorphic properties of well-known cryptosystems.

We designed, implemented and evaluated the performance of our algorithms on real mobile devices. We showed that our solutions preserve user preference privacy and have acceptable performance in a real implementation. Moreover, we extended the proposed algorithms to include cases where users have several prioritized locations preferences. Finally, based on an extensive user-study, we showed that the proposed privacy features are crucial for the adoption of any location sharing or location-based applications.

Bibliography

[1] (2011, Nov.). *Facebook Statistics* [Online]. Available: http://www.facebook.com/press/info.php?statistics

[2] (2011, Nov.). *Facebook Deals* [Online]. Available:http://www.facebook.com/deals/

[3] E. Valavanis, C. Ververidis, M. Vazirgianis, G. C. Polyzos, and K. Norvag, “MobiShare: Sharing context-dependent data & services from mobile sources,” in *Proc. IEEE/WIC Int. Conf. WI*, Oct. 2003, pp. 263–270.

[4] (2011). *Microsoft Survey on LBS* [Online]. Available: http://go.microsoft.com/?linkid=9758039

[5] (2011, Nov.). *Orange Taxi Sharing App* [Online]. Available: http://event.orange.com/default/EN/all/mondial

[6] (2011). *Let’s Meet There* [Online]. Available: http://www.letsmeetthere.net/

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

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

[9] J. Freudiger, M. Jadliwala, J.-P. Hubaux, V. Niemi, P. Ginzboorg, and I. Aad, “Privacy of community pseudonyms in wireless peer-to-peer networks,” *Mobile Netw. Appl.*, vol. 18, no. 3, pp. 413–428, 2012.

[10] (2011, Nov.). *Please Rob Me* [Online]. Available: http://pleaserobme.com/