International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Analysis of Security in Optimal Meeting Location Determination

Mr. Mittapalli.Sai Kumar
M.Tech Student Department of CSE
Aurora's Technological And Research Institute
Email id: saik7841@gmail.com

Mrs. **S.Swapna**
Assistant Professor Department of CSE & IT
Aurora's Technological And Research Institute
Email id: vooreswapna205@gmail.com

Abstract:

Equipped with state-of-the-art smart phones and mobile devices, today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. These applications often rely on current (or preferred) locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current (or preferred)locations to the service provider or to other, possibly un-trusted, users. In this paper, we propose privacy-preserving algorithms for determining an optimal meeting location for a group of users. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In order to study the performance of our algorithms in a real deployment, we implement and test their execution efficiency on Nokia smart phones. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location based services and the usability of the proposed solutions.

Index Terms—Mobile application; oblivious computation; privacy

I. INTRODUCTION

THE rapid proliferation of smartphone 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 [4], 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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

global telecom operator, where smartphone 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. 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.

Without effective protection, even sparse 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. Recent user studies show that end-users are extremely sensitive about sharing their location information. Our study on 35 participants, including students and non-scientific staff, showed that nearly 88% of users were not comfortable sharing their location information. Thus, the disclosure of private location in any Location-Sharing-Based Service (LSBS) is a major concern and must be addressed.

II SYSTEM ANALYSIS

(A) 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.

(B) Disadvantages:

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.

(C) 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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

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.

(D) ***Advantages****:*

We address the privacy issue in LSBSs by focusing on a specific problem called the *Fair Rendez-Vous 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.

III SYSTEM ARCHITECTURE

We take a system consists of two entities:

(i) a set of users1 (or mobile devices) $\mathbf{U = \{u_1, \ldots, u_N\}}$ and

(ii) a third-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.

Every mobile device is able to communicate with the LDS by through 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. Here, We take a two-dimensional coordinate system, but the system that we proposed is general enough and can be easily extended to other higher dimensional coordinate systems. 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.

FRVP algorithm is executed by the LDS, on the inputs it receives from the users in order to compute the FRV point. And these LDS are able to do public-key cryptographic functions. For instance, a common public-key infrastructure using the RSA cryptosystem could be employed. Let $\boldsymbol{K_p}^{\boldsymbol{LDS}}$ be the public key, certified by a trusted CA, and $\boldsymbol{K_s}^{\boldsymbol{LDS}}$ the corresponding private key of the LDS. $\boldsymbol{K_p}^{\boldsymbol{LDS}}$ is 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 $\boldsymbol{K_s}^{\boldsymbol{LDS}}$. This ensures message confidentiality and integrity. For simplicity, we do not explicitly show the cryptographic operations involving LDS's public/private key.

A. Threat Model

1) *Location Determination Server:* The primary type of LDS adversarial behavior that we want to protect against is an *honest-but-curious* or semi-honest adversary, where the LDS is assumed to execute the algorithms correctly, i.e., take all the inputs and produce the output according to the algorithm, but is not fully trusted. It may try to get users' location preferences from the received inputs, the intermediate results and the produced outputs.

In most practical settings, where service providers have a commercial interest in providing a faithful service to their customers, the assumption of a semi-honest LDS is generally sufficient. Given this goal of protecting against a semi-honest LDS, we will later also analyze how our proposed solutions fair against certain *active attacks*, including collusion with users and fake user generation.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

2) *Users:* Our main goal is to protect against semi-honest participating users who may want to learn the private location preferences of other users from the intermediate results and the output of the FRVP algorithm. This attack can be taken as a *passive attacks*. As user inputs are encrypted with the LDS's public key K_P^{LDS} , we can guarantee that our data is secure.

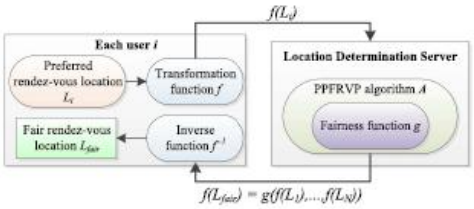

Fig. 1. Functional diagram of the PPFRVP protocol.

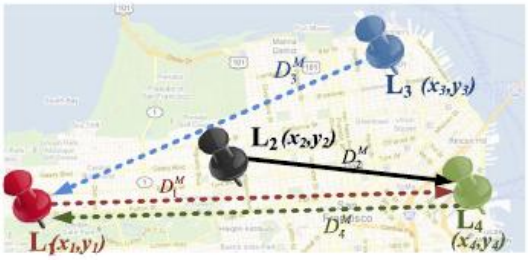

Fig. 2. PPFRVP scenario, where the fairness function is g = argmin$i$ (D_i^M). The dashed arrows represent the maximum distance D_i^M from each user u_i to any user j != i, whereas the solid line is the minimum of all such maximum

IV. PPFRVP PROBLEM FORMULATION

Here, we worked on problem of finding a rendezvous point among a set of user-proposed locations, such that

i. the rendezvous point is *fair* (as defined in Section IV-A) with respect to the given input locations,
ii. each user learns only the final rendezvous location and
iii. no participating user or third-party server learns private location preference of any other user involved in the computation.

We refer to an algorithm that solves this problem as *Privacy-Preserving Fair Rendez-Vous Point (PPFRVP)* algorithm. In general, any PPFRVP algorithm A should accept the inputs and produce the outputs, as described below.

- *Input*: transformation f of private locations $Li : f(L_1) \| f(L_2) \| \ldots \| f(L_N)$. where f is a secret-key based encryption function such that it is hard (success with only a negligible probability) to determine the input L_i without knowing the secret key, by just observing $f(L_i)$.
- *Output*: an output $f(L_{fair}) = g(f(L_1), \ldots, f(L_N))$, where g is a fairness function and $L_{fair} = (x_l, y_l) \in N^2$ is the fair rendez-vous location such that it is hard for the LDS to determine L_{fair} by just observing $f(L_{fair})$. Given $f(L_{fair})$, each user should be able to compute $L_{fair} = f-1(f(L_{fair}))$ by using a decryption routine and the shared secret key.

The functional diagram of the PPFRVP protocol is represented in figure 1, where an LDS executes the PPFRVP algorithm A . The fairness function g can be defined in several ways, depending on the preferences of users or policies. Fairness function that minimizes the maximum displacement of any user to all other locations is represented in figure 2. This function is globally fair and can be easily extended to include additional constraints and parameters.

V IMPLEMENTATION MODULES

(A) 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.*

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

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-linkability 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* .

(B) 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.

(C) 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.

(D) Privacy Under Multiple Dependent Execution:

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 AND FUTURE WORK

The privacy issue is addressed in this work, in the Fair Rendezvous Problem (FRVP). Our solutions are based on the homomorphic properties of well-known cryptosystems. We designed, implemented and evaluated the performance of our algorithms and showed that our solutions preserve user preference privacy and have acceptable performance. Moreover, we extended the proposed algorithms to include cases where users have several prioritized locations preferences. Finally, based on user-study, we proved that our proposed security features are crucial for the adoption of any location sharing or location-based applications.

REFERENCES

[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/