Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Survey Paper on Privacy-Preserving Optimal Meeting Location on Mobile Devices

**Samta M. Jain**
Department of Computer Technology
Rajiv Gandhi College of Engg. Research & Technology
Chandrapur, Maharashtra, India

**P S. Kulkarni**
Hod, Department of Information Technology,
Rajiv Gandhi College of Engg. Research &Technology,
Chandrapur, Maharashtra, India

***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)* algorithm.

## II. LITERATURE SURVEY

### A. *DBGlobe: A Service-Oriented P2P System for GlobalComputing*

The challenge of peer-to-peer computing goes beyond simple file sharing. In the DBGlobe project, we view the multitude of peers carrying data and services as a super-database. Our goal is to develop a data management system for modeling, indexing and querying data hosted by such massively distributed, autonomous and possibly mobile peers. We employ a service-oriented approach, in that data are encapsulated in services. Direct querying of data is also supported by an XML-based query language. In this paper, we present our research results along the following topics: (a) infrastructure support, including mobile peers and the creation of context-dependent communities, (b) metadata management for services and peers, including location-dependent data, (c) filters for efficiently routing path queries on hierarchical data, and(d) querying using the AXML language that incorporates service calls insideXMLdocuments.

DBGlobe is an ongoing project. Our future plans include among others appropriate notions ofdata consistency as well as providing a more systematic treatment of updates.

 

### *B. Privacy of Community Pseudonyms in WirelessPeer-to-Peer Networks*

Wireless networks offer novel means to enhance social interactions.In particular, peer-to-peer wireless communications enable directand real-time interaction with nearby devices and communities andcould extend current online social networks by providing complementary services including real-time friend and community detection and localized data sharing withoutinfrastructure requirement.After years of research, the deployment of such peer-to-peer wire-less networks is finally being considered. A fundamental primitives the ability to discover geographic proximity of specific communitiesof people (e.g, friends or neighbors). To do so, mobile devicesmust exchange some community identifiers or messages. We investigate privacy threats introduced by such communications, in particular, adversarial community detection. We use the general con-cept of community pseudonyms to abstract anonymous community identification mechanisms and define two distinct notions of com-munity privacy by using achallenge-responsemethodology. Anextensive cost analysis and simulation results throw further light on the feasibility of these mechanisms in the upcoming generationof wireless peer-to-peer networks.

In this paper, we considered the problem of community privacyin peer-to-peer wireless networks and evaluated privacy risks of in-formation sharing within communities in such networks. Identifying the need to protect community privacy, we proposed a frame-work based on challenge-response games to study it. An interesting outcome of the framework is the analytical relation obtainedbetween community anonymity and community unlinkability. Therelation between these two properties was previously studied.To the best of our knowledge, we are the first to analytically relate these properties.By means of simulations, we evaluated the privacyprovided bydifferent pseudonym-based community privacy-preserving schemes.Our results throw light on the relationship between community pseudonym-based and secret handshake schemes: shrinking the number of possible community pseudonyms significantly reduces the achievableprivacy. Hence, it is not advisable to cycle through a small set ofpseudonyms with secret handshakes. This result illustrates the delicate trade-off between theachievable community privacy and thecost of community pseudonym schemes. Our analysis enables sys-tem designers to tune their shrunk scheme to a desired privacy levelby, for example, regularly changing the set of community pseudonyms. We also showed that reusing pseudonyms across communities (Hints) can provide a good cost/privacy trade-off and demonstrated thatk-anonymous schemes are, at best, detrimental to com-munity privacy. In the future, we intend to investigate other communication models and, by means of practical implementations,study the extra overhead introduced by community pseudonym schemes.

### *C. Quantifying Location Privacy:TheCaseofSporadicLocationExposure*

Mobile users expose their location to potentially untrustedentities by using location-based services. Based on the frequency of location exposure in these applications, we divide them into two main types:Continuous andSporadic. These two location exposure types lead to different threats. For example, in the continuous case, the adversary cantrack users over time and space, whereas in the sporadic case, his focusis more on localizing users at certain points in time. We propose a systematic way to quantify users' location privacy by modeling both thelocation-based applications and the location-privacy preserving mechanisms (LPPMs), and by considering a well-defined adversary model.This framework enables us to customize the LPPMs to the employedlocation-based application, in order to provide higher location privacyfor the users. In this paper, we formalizelocalizationattacks for thecase of sporadic location exposure, using Bayesian inference for HiddenMarkov Processes. We also quantify user location privacy with respect tothe adversaries with two different forms of background knowledge: Thosewho only know the geographical distribution of users over the consideredregions, and those who also know how users move between the regions(i.e., their mobility pattern). Using the Location-Privacy Meter tool, weexamine the effectiveness of the following techniques in increasing theexpected error of the adversary in the localization attack: Location obfuscation and fake location injection mechanisms for anonymous traces

We propose, to the best of our knowledge, the first formal framework for quantifying location privacy in the case where users expose their location sporadically. We formalize sporadic location-based applications. Using this formalization, wemodel various location-privacy preserving mechanisms, such as location obfuscation and fake-location injection. Formalizing both location-based applications and location-privacy preserving mechanisms in the same framework enables usto design more effective protection mechanism that are appropriately tailored toeach location-based service. We also establish an analytical framework, based onBayesian inference in Hidden Markov Processes, to perform localization attackson anonymized traces (for adversaries with differentbackgroundknowledge).The results obtained from the simulations of the attacks on mobility traces un-veil the potential of various mechanisms, such as the location obfuscation, thefake-location injection, and anonymization, in preserving location-privacy of mobile users.

### *D. Privacy in Mobile Computing forLocation-Sharing-Based Services*

Location-Sharing-Based Services (LSBS) complement Location-Based Services by using locations from a group of users, and not just individuals, to provide some contextualized service based on the locationsin the group. However, there are growing concerns about the misuse oflocation data by third-parties, which fuels the need formore privacycontrols in such services. We address the relevant problem of privacy. In LSBSs by providing practical and effective solutions to the privacyproblem in one suchservice, namely the fair rendezvous point (FRVP)determination service. The privacy preserving FRVP (PPFRVP) problem is general enough and nicely captures the computations and privacyrequirements in LSBSs. In this paper, we propose two privacy-preservingalgorithms for the FRVP problem and analytically evaluate their privacyin both passive and active adversarial scenarios. We study the practicalfeasibility and performance of the

 

proposed approaches by implementing them on Nokia mobile devices. By means of a targeted user-study, weattempt to gain further understanding of the popularity, the privacy andacceptance of the proposed solutions

In this work, we address the problem of privacy in LSBS by providing practical and eff-ective solutions to one such popular and relevant service. The PPFRVPproblem captures the essential computational and privacy building blocks presentin any LSBS offered on mobile devices. We designed, implemented on real mo-bile devices and evaluated the performance of our privacy-preserving protocols16 for the fair rendezvous problem.Our solutions are effective in terms of privacy, have acceptableperformance, and do not create additional overhead forthe users. Moreover,our user-study showed that the proposed privacy features are crucial for the adoption of any such application, which reinforces the needfor further exploration in privacy of LSBservices. To the best of our knowledge,this is the first such effort in this direction.

### *E. Secure Actor Directed Localization in Wireless Sensorand Actor Networks*

Wireless sensor and actor networks are fully automated. Actor nodes are inducted to communicate with sensor nodes directly andreduce the communication delay caused by base station or sink nodes. Sometimes, the actor node is directly accessible withoutthe involvement of any control room. The actor node is responsible for taking a prompt action against the reported event by asensor node. For secure communication, it is essential that sensor and actor nodes be aware of their existing location and the data must be encrypted before transmission. Due to energy constraints, secure localization in wireless sensor networks is a hot issue.To date, the researchers have proposed many approaches for localization of sensor nodes in the network. In this paper, we providenew insights for secure actor directed localization technique in wireless sensor and actor networks. A secure connectivity basedlocalization (CBL) approach for sensor and actor nodes localization is presented. The proposed approach helps to locate a sensornode efficiently and effectively. We have also decreased the possibility of attacks and the registration of attacker nodes with otherlegitimate nodes in the network. The proposed technique prevents man-in-the-middle attacks and securely delivers data to thedestination.

In this paper we proposed a secure mechanism for localization of sensor nodes in wireless sensor networks. Using anencryption algorithm for secure data delivery and registration of sensors with anchor node, we effectively minimizeand block the external attacks. After simulation results, weconclude that efficient localization in sensor networks can begreatly enhanced by the understanding of both connectivityof sensor nodes and to which nodes they are not connected.The mechanism shows a particular area in which a node canbe localized and we caneasily find it there. Once the anchor node locates its own position, the sensor nodes are able to localize each other. This approach is initiated by the anchornode having higher resources than sensor node; therefore, itwill reduce energy consumption as well as increase networks lifetime. Howeverthefutureworkistostoptheinternalattacks and reduce the number of compromised sensor nodesin the network.

### *F. MILC: A secure and privacy-preserving mobile instantLocator with chatting*

The key issue for any mobile application orservice is the way it is delivered and experienced by users,who eventually may decide to keep it on their softwareportfolio or not. Without doubt, security and privacy haveboth a crucial role to play towards this goal. Very recently,Gartner has identified the top ten of consumer mobile applications that are expected to dominate the market in thenear future. Among them one can earmark location-basedservices in number 2 and mobile instant messaging innumber 9. This paper presents a novel application namelyMILC that blends both features. That is, MILC offers usersthe ability to chat, interchange geographic co-ordinates andmake Splashes in real-time. At present, several implementations provide these services separately or jointly, but noneof them offers real security and preserves the privacy of theend-users at the same time. On the contrary, MILC providesan acceptable level of security by utilizing both asymmetricand symmetric cryptography, and most importantly, put theuser in control of her own personal information and her private sphere. The analysis and our contribution are three-fold starting from the theoretical background, continuing tothe technical part, and providing an evaluation of the MILCsystem. We present and discuss several issues, including thedifferent services that MILC supports, system architecture,protocols, security, privacy etc. Using a prototype implemented in Google's Android OS, we demonstrate that theproposed system is fast performing, secure, privacy-preserving and potentially extensible.

Mobile applications are expected to mushroom over thenext few years. This is driven by several strong factorslike the growing interest in smart-phones and theinvolvement of Internet players into the mobile realm. This is further supported by modern networkscapabilitiesand developers capitalizing open platforms. Forinstance, the continuous success of the iPhone and theadoption of Google's Android operating system by mobilehardware vendors and service providers stimulate thepenetration of smart-phones into the market and thedemand for sophisticated mobile services. In this context,mobile social networking applications gain popularity andincrease the volume of their users rapidly. However, sofar, most of them have failed to deliver truly secure andprivacy-preserving services to their users. Everyone wouldagree that anyone who participates in a virtual communityneeds to rest assure that any information she sends andreceives remains confidential and that her private sphere isnot violated without her consent. In this paper we present the MILC system which isclassified under the umbrella of mobile social networkingapplications. Specifically, MILC integrates in private orClosed communities of scope individuals that participate inthe community, mainly for educational reasons (students communities, research groups etc.). MILC tries to addressthe aforementioned issues by (a) utilising both asymmetricand symmetric cryptography to provide a high level ofsecurity to its users, and (b) respecting end-user privacy byputting the user in control of what private information isrevealed to other parties and under what circumstances. Weprovide a detailed description of the MILC prototypecomponents, discussing their functionality and

 

analyzingtheir aspects. We also demonstrate that MILC is lightweightin terms of service times. Also, we believe that our designcan be used as a template for anyone interested in building, expanding and deploying a MILC-like system. As a statement of direction, we are currently working onenhancing MILC to support and further improve distanceservices offered to the academic community.

### *G. Enhanced Flexibility for HomomorphicEncryption Schemes via CRT*

The Chinese Remainder Theorem (CRT) has numerous applications including in cryptography. In a striking example of this utility, we demonstrate how the CRT facilitates making one additive homomorphic encryption scheme viable and making another more exible. Firstwe show that theCRT may be used to turn an intractable problem intoa tractable one. Specically, using the CRT to replace a single group element by a logarithmic number of elements in the same group, we lay thefoundation for additively homomorphic encryption schemes using wellknownandpreviously deployed primitives. Our solution is shown to besecure and quite general in nature. We present a simple technique forElGamal-type encryption schemes which facilitates encryption in an additively homomorphic manner. Secondly we apply the CRT to a previous encryption scheme proposed by Boneh, Goh and Nissim that supportefficient homomorphic evaluations of 2-DNF circuits . One drawback mentioned was a restriction on the size of the output message space{ prompting an open problem posed by the authors. Again employing the CRT, we devise an elegant modification in which we solve the problem,supporting arbitrary output sizes.

We proposed a simple solution to the pervasive bottleneck in additive homomorphic encryption schemes based on the hardness of the DLP. We employed theCRT to replace one discrete logarithm problem in a large space by several similar problems in a more tractable search space while retaining full security. Thisyields, the first practical elliptic curve-based additive homomorphic encryption scheme. More generally, our CRT technique makes discrete logarithm problemsasymmetric, thereby lending itself as a tool to build a number of practical DLPbased additive homomorphic schemes. As an example, ourCEG-ECCscheme is shown to be almost 4 times fasterthan Paillier scheme on the encryption side while maintaining comparable security. This maybe useful in applications where encryption is used much moreoften than decryption. A key feature of the proposed scheme is its exible message space. Solely for the sake of security, the Paillier encryption scheme alwaysrequires 4096-bit operations, even for single bit computations. In contrast, the CEG-ECCscheme can be customized to meet the message space demands of anyapplication; the lower limit is set by the diculty of the ECC discrete logarithmproblem. But the message space of the proposed scheme can be easily expandedby simply adding more CRT components. As the number of components grows only logarithmically with the message space, the performance impact is quite manageable. We also found the CRT approach valuable as a way to solve an open problemin [4] where Boneh, Goh and Nissim describe a scheme which homomorphically evaluates 2-DNF formulas. In their paper, the need to perform a discrete logarithm as part of the decryption process seemed to place a strict limitation on thesize of their message space. The Chinese Remainder Theorem variant CRT-BGN maintains security while replacing this hard discrete logarithm computation with t discrete logarithm problems in a completely manageable search space.

### *H. A Factoring and Discrete Logarithm basedCryptosystem*

This paper introduces a new public key cryptosystem based on twohard problems: the cube root extraction modulo a composite moduli(which is equivalent to the factorisation of the moduli) and the discretelogarithm problem. These two hard problems are combined during thekey generation, encryption and decryption phases. By combining theIFP and the DLP we introduce a secure and efficient public key cryptosystem. To break the scheme, an adversary may solve the IFP andthe DLP separately which is computationally infeasible. The key generation is a simple operation based on the discrete logarithm modulo composite moduli. The encryption phase is based both on the cuberoot computation and the DLP. These operations are computationallyefficient.

We successfully introduce a new efficient and secure cryptosystem by combining two cryptographic assumptions namely the cube root extraction and thediscrete logarithm problem modulo a composite integer. It's well known that most of the existing schemes are based on single problems and if an adversarycould find an algorithm to solve the related problem the scheme is broken. Ourscheme is prevented from this problem since it's based on two hard problems.An adversary may break it if he is able to solve simultaneously the two related problem which is very unlikely to happen. On the other hand the new scheme is as efficient as the El Gamal one and should be an alternative to the othercryptosystems.

### *I. The Advantages of Elliptic Curve Cryptography for wireless Security*

This article provides an overview of ellipticcurves and their use in cryptography. The focusis on the performance advantages to be obtainedin the wireless environment by using ellipticcurve cryptography instead of a traditional cryptosystem like RSA. Specific applications tosecure messaging and identity-based encryptionare discussed.

Over the last five years, elliptic curve cryptography has moved from being an interesting theo-retical alternative to being a cutting edgetechnology adopted by an increasing number of companies. There are two reasons for this newdevelopment: one is that ECC is no longer new, and has withstood a generation of attacks; second, in the growing wireless industry, its advan-tages over RSA have made it an attractivesecurity alternative.Wireless Internet mail industry leaders such as Qualcomm have embraced ECC, as well asother major companies in the wireless industrysuch as Motorola, Docomo, and RIM. Majorcomputer companies such as IBM, Sun Microsystems, Microsoft, and Hewlett-Packard are allinvesting in ECC. The U.S. government is back-ing the use of ECC as well, with NSA creatingthe security requirements for wireless devicesconnecting to the military, and NIST providingstandardized curves for use in a range of

 

applications of ECC. Smartcard companies such asGemplus are also using ECC to improve theirproducts' security.Wireless devices are rapidly becoming moredependent on security features such as the ability to do secure email, secure Web browsing, andvirtual private networking to corporate networks,and ECC allows more efficient implementationof all of these features.

### *J. Older Adults Engage in Privacy Enhancing Behaviors in aHome Monitored WithRobotsorCameras*

In this paper, we describe the results of an experimental study in which older adult participants interacted with three monitoring technologies designed to support older adults' ability to age in place in their own home—a camera, a stationary robot, and a mobile robot. The aim of our study was to evaluate users' perceptions of privacy and their tendencies to engage in privacy enhancing behaviors (PEBs) by comparing the three conditions. We expected participants to engage in more PEBs when they were interacting with the mobile robot, since it provided embodied cues of ongoing monitoring. Surprisingly, we found the opposite to be true the camera was the condition in which participants performed more PEBs. We describe the results of quantitative and qualitative analyses of our survey, interview, and observational data and discuss the implications of our study for human-robot interaction, the study of privacy and technology, and the design of assistive robots for monitoring older adults.

This paper presented the results from an experimental study of the privacyrelated behaviors and perceptions of older adults participants interacting with three types of monitoring technology: a camera, a stationary robot (with camera), and a mobile robot (with camera). We wereparticularly interested in seeing how older adults reacted to the two robots in comparison to the camera, as there has been little empirical research on privacy behaviors in the context of human-robot interaction. While HCI researchers have investigated privacy with respect to manytechnologies (e.g., mobile, cameras, internet, social networking) our work is the first to consider the notion of embodied and interactive monitoring technologies, such as robots. The literature in HRI has so far not delved into empirical research on privacy behaviors around robots, but one of the expectations researchers have put forth is that robots might enable users to protect their privacy more effectively, since they are physically larger than cameras, their movements are obvious to users and they can be asked to move out ofthe room, and thus evadedwhen desired

.Our study specifically addressed this area at the intersection of HRI and HCI, looking at embodiment in respect to privacy. We hypothesized that an embodied, mobile monitoring technology would increase participants 'use of PEBs, but we found the opposite to be truefewer participants engaged inPEBsaround robots. While we discussed potential explanations for this finding, more research is needed to evaluate these and other explanations. In the future, we propose to do more research to find out why this is the case, as we were only able to get a partial understanding from user comments in final interviews.

## III. 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.

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.

## IV. PROPOSED SOLUTION

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.We first Formulate the FRVP problrm as k-center problem and then analytically outline the privacy requirment of the participants with respect to each other and respect to third party service provider.

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. Our proposed algorithms take advantage of the homomorphic properties of well-known cryptosystems, such as BGN, ElGamal and Paillier, in order to privately compute an optimally fair rendez-vous point from a set of user location preferences.

## V. CONCLUSION

This paper proposes the privacy issue in FRVP. Our method is based on the homomorphic properties of well-known cryptosystems,such as BGN, ElGamal and paillier, in order to privetly compute an optimally fair rendez-vous point from a set of users location preferences. Proposed solutions will preserve user preferences privacy and have acceptable performance in real implementation.It may encourage users to stop revealing sensitive information to third-parties and untrusted users,such as their home and work location and agree to privacy preserving mechanism.

 

**REFERENCE**

[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/

 