International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 6 (Nov-Dec 2016), PP.68-71

A Study on Determining Optimal Meeting Locations

[1] Abhijeet Jagadale, [2]Dipak Chavan, [3]Akshay Jadhav, [4]Prashant Almalkar
[1,2,3,4] UG Student, Dholepatil College of Engineering, Wagholi, Savitribai Phule Pune University
[1]Professor, Computer Department, Dholepatil College of Engineering, Wagholi, Savitribai Phule Pune University
[1] abhijagadale84@gmail.com, [2] dipakchavan68@gmail.com, [3] akshay72558@gmail.com, [4] prashantalmalkar91221@gmail.com,
[1] manishasingh4314@gmail.com

Abstract— **There are lots of smart-phones and mobile devices are continuously increases and fully interconnected to city or town population is more and more addicted to these appliance to develop and arrange their daily lives. These applications preferred locations of particular users or a group of users to create the required service, that jeopardizes their privacy; users don't essentially wish to expose their preferred or current position to the service provider or to different, presumptively untrusty users. In this paper, we tend to offer secrecy-conserving algorithms for deciding Associate in nurturing best meeting area for a group or bunch of users. We try to execute a radical privacy analysis by formally measuring secrecy-loss of the projected approaches. So as to verify the operation of our algorithms during a genuine readying, we tend to improve and notice at their execution capability on Nokia smart-phones. By the study of targeted users we try to plan to get Associate in nurturing insight into the privacy-cognizance of users in area based mostly services and also the ability to use the projected solutions.**

Keywords— **Optimal Locations, Privacy, Global Positioning System (GPS), Position Based Servers, oblivious computation, Mobile application.**

I. Introduction

Speedy teemingness of smart-phone technology in city profession has enabled cell-phone users to use context aware services on their system or devices. Facilities providers take benefit of this dynamic and growing technology landscape by proposing advance context-dependent services for cell subscribers. Location based Services (LBS), for eg- are used by billions of mobile subscribers every day to get location-specific information. [1].

There are two causes in cell-phone environment to challenging location secrecy preservation. Interception of Wireless communications are easy e.g. eavesdropper can store transmitted data of cell-phone users at some public place. Since people are publicly notice, context information can easily be get from their conversation. As a result, partial trajectory data related with a user's real identity is necessarily exposed to the eavesdropper. Second, the limited resources of cell-phones greatly bound secrecy raising Technologies one could deploy and apply in wireless network. Current solutions reply on simple rule to hide the real identity of a mobile phone user from a passive opposer, rather than complex cryptographic technologies.

Location check-ins and location sharing are two popular characteristics of location-based services. Inspection in an area, users can deal their present location with friends and family or find location-specific services from third-party supplier. The obtained service does not depend on the area of other users.

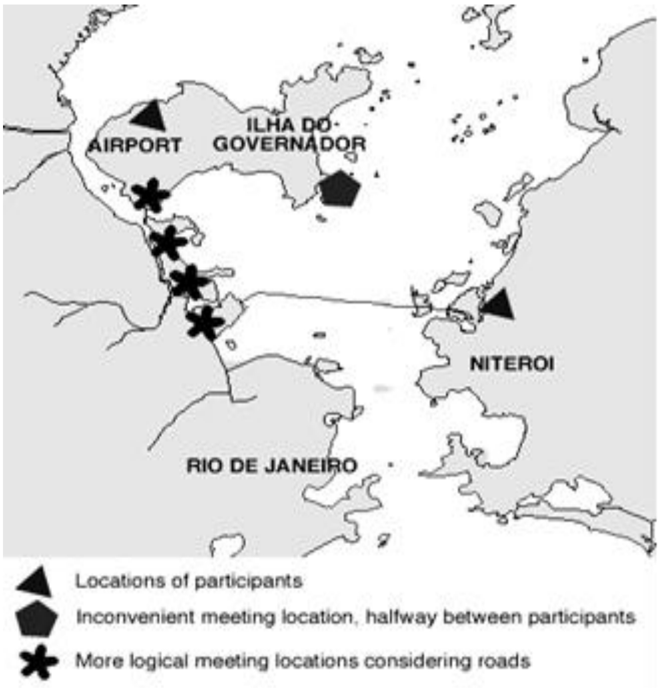
AIRPORT
ILHA DO GOVERNADOR
NITEROI
RIO DE JANEIRO
Locations of participants
Inconvenient meeting location, halfway between participants
More logical meeting locations considering roads

Fig 1. Optimization for geographic centers might miss logical meeting points.

The another types of (LBS) location-based services, which depend on sharing of locations by a bunch of users in order to receive some service for the whole bunch or group, are also seemly famous. Secrecy of a user's area or location preferences, compare to other users and the third-party service supplier, is a difficult matter in such location-sharing-based applications.

For example, this type of information can be used to distract users and their availableness, to search their preferences or to recognize their social networks. A third-party service supplier could easily guess home or work location more than one users who use their service on regular basis in the application of texi-sharing. Without effective security, if the stored data is passed in an unknown fashion with corporate peoples, which could have dangerous result on the users' social, personal and financial life.

Literature Survey

A. DBGlobe: A Service-Oriented P2P System for Global Computing.

The challenge of device to device computing goes beyond simple file sharing. We see the multitude of peers carrying data and services as a super-database in the DBGlobe project. Our target is to create a data management system for indexing, modeling and querying data hosted by such widely distributed, free and possibly mobile peers. We apply a service-oriented to come near, in that data are capsulize in services. Directly querying of data is also supported by an XML query language. Now in this section we show our research output along the following topics: (a) infrastructure support, with mobile peers and the making of context-dependent communities, (b) metadata system management for services and peers, including location-dependent information, (c) filters for frequently routing path problems on hierarchical data, and (d) querying using the AXML language that incorporates service calls in the XML documents.

Here, ongoing project is an DBGlobe and the future plans with others applicable notions of data flexibility as well as giving a more diplomatic treatment of updates.

A. Secrecy of Community Pseudonyms in Wireless Peer-to-Peer Networks

Wireless networks give the novel means to improve social relations. In particular, line-to-line wireless communications activate, direct and real-time interaction with nearly devices and communities and could improve current online social networks systems by giving correlative services adding real-time community detection and friend and localized data sharing without requirement of infrastructure. After more years of research, the result of such mobile to mobile wire-less networks is finally being allowed. A fundamental primitives the ability to discover geographic proximity of specific communities of people (e.g, friends or neighbors). So that, cell phone devices must interchange some community identifiers or messages. We inspect secrecy threats developed by such systems communications, in particular, adversarial community detection. We use the idea of community pseudonyms to abstract anonymous community identification mechanisms and explain two distinct notions of community secrecy by using a challenge-response techniques. A wide cost investigation and duplicate results throw further light on the consistency of these mechanisms in the further coming generation of wireless device to device networks. In this paper, we included the problem of community secrecy in line-to-line wireless networks and look over secrecy risks of information sharing within communities in such networks. Finding the need to safe community secrecy, we proposed a frame-work based on great challenge-response games to study it. An impressive result of the framework is the analytical relation received between community unlink ability and community anonymity. The relation between these two properties was studied previously. To the study of our knowledge, we are the one to analyse how to relate these properties. By means of simulated results, we evaluate the secrecy provided by different pseudonym-based community secrecy-conserving schemes. Our output results throw light on the relationship between community pseudonym-based and secret handshake schemes: shrinking the number of possible community pseudonyms significantly reduces the achievable secrecy. Hence, it is not applicable to cycle through a small set of pseudonyms with secret handshakes. This result describe the soft trade-off between the obtainable community secrecy and the cost of community pseudonym schemes. Our research enables system designers to tune their compress or shrunk scheme to a desired secrecy level, for example, daily changing the set of community pseudonyms. We also reviewed that reusing pseudonyms across communities (Hints) can provide a good cost/secrecy trade-off and exposed that anonymous schemes are at best harmful to community secrecy. In the future, we intend to inspect other communication design and by means of practical performance, study the extra overhead introduced by community pseudonym schemes.

B. Quantifying Location Privacy: The Case of Sporadic Location Exposure

Mobile users shows their area location to potentially unauthorized entities by using location-based services system. Based on the no. of times of sharing location in these applications, we cut them into mainly two types:

One is Continuous and the other is infrequent.

These two sharing location types lead to different hazards. Lets an example, in the continuous case the attacker can find users over time and space, whereas in the infrequent case, his object is more on localizing users at few points in time. We introduce a analytical way to estimate users location secrecy by modeling both the location-based applications and the location-privacy preserving mechanisms (LPPMs), and by mentioning a well-defined working model. This framework enables us to customize the LPPMs to the employed location-based application, in order to furnish higher location secrecy for the users. In this paper, we illustrate localization attacks for the case of some sharing location, using Bayesian inference for Hidden Markov Processes. We also evaluate user location secrecy with respect to the attackers with two different way of background knowledge: Those who know the geographical structure distribution of users over the mentioned regions or area, and those who also know how users move out between the different regions (i.e., their mobility pattern system). Using the Location-secrecy Meter tool, we check the effectualness of the following techniques in increasing the likely error of the adversary in the localization attack: Location breaking and fraud location injection mechanisms for anonymous traces We propose, to the best of our idea, the first formal framework for evaluating location secrecy in the case where users display their location sporadically. We validate irregular location-based applications. By using this formalization, we model different location secrecy conserve mechanisms, such as location obfuscate and fraud-location area injection. Formalizing both area location-based applications and location-secrecy conserving mechanisms in the same framework active us to design more effective safe mechanism that are applicable tailored to each location-based service. We also built an logical framework, based on Bayesian inference in Hidden Markov Processes, to perform localization fire on anonymized traces (for attackers with different background knowledge). The results get from the simulations of the attacks on mobility traces un-veil the strength of different mechanisms, such as the location breaking, the false-location injection, and anonymization, in conserving location-secrecy of cell phone users.

D. Privacy in Mobile Computing for Location-Sharing-Based Services

Location-Sharing-Based Services (LSBS) usually Location-Based Services by using locations from a bunch of users, and not just private, to share few contextualized facility based on the locations in the group. However, there are improving task about the misuse of location data by third-parties, which fuels the need for more secrecy secures in such services. We relate the suited problem of privacy. In LSBSs by giving practical and capable solutions to the secrecy problem in one such service, namely the fair rendezvous point (FRVP) determination service. The secrecy conserving FRVP (PPFRVP) problem is general sufficient and nicely captures the computations and secrecy requirements in LSBSs. In this paper, we take two secrecy-conserving algorithms for the FRVP problem and logically describe their privacy in both active and passive adversarial scenarios.

We study the feasibility and execution of the proposed approaches by implementing them on Nokia mobile phone devices. By the targeted user-survey, we effort to gain further understanding of the popularity, the secrecy and acceptance of the proposed solutions. In this work, we notify the problem of secrecy in LSBS by giving practical and effective solutions to one such popular and relevant service. The PPFRVP problem looks the essential computational and secrecy building blocks present in any LSBS offered on mobile devices. We architect and implemented on real mobile devices and analyse the performance of our privacy-preserving protocols16 for the fair rendezvous problem. Our outputs are effective in terms of secrecy, have acceptable performance, and do not make additional overhead for the users. Moreover, our user-survey showed that the proposed secrecy features are important for the acceptance of any such application, which reinforces the need for further exploration in secrecy of LSB services. To the best of our knowledge, this is the first such type effort in this direction.

E. Secure Actor Directed Localization in Wireless Sensor and Actor Networks

Wireless sensor network and actor networks are both fully automated. Actor nodes are initiate to communicate with sensor nodes directly and reduce the communication time caused by base station or sink nodes. Sometimes, the actor node is directly access without the adding of any other control room. The actor node is head for taking a prompt action against the reported event by a sensor node. For safe communication, it is important that sensor and actor nodes be aware of their existing location and the data must be encrypted before execution. Due to energy constraints, safe 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 provide new insights for secure actor directed localization technique in wireless sensor and actor networks. A secure connectivity based localization (CBL) approach for sensor and actor nodes localization is presented. The proposed approach helps to locate a sensor node efficiently and effectively. We have also decreased the possibility of attacks and the registration of attacker nodes with other legitimate nodes in the network. The proposed technique prevents man-in-the-middle attacks and securely deployed data to the destination. In this paper we proposed a safe mechanism for localization of sensor nodes in wireless sensor networks. Using an encryption algorithm for safe data deployment and registration of sensors with anchor node, we effectively minimize and block the external attacks. After simulation results, we conclude that efficient localization in sensor networks can be greatly enhanced by the understanding of both connectivity of sensor nodes and to which nodes they are not connected. The mechanism shows a particular area in which a node can be localized and we can easily 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 anchor node having higher resources than sensor node; therefore, it will reduce energy consumption as well as increase networks lifetime. However the future work is to stop the internal attacks and reduce the number of compromised sensor nodes in the network.

CONCLUSIONS

Thus the paper carries out the thorough survey on location privacy preserving techniques and optimal meeting location determination techniques. The various techniques previously proposed do not provide

both the things i.e. privacy preserving feature and the optimal meeting location calculation in organization meeting environments. Thus it is essentials to proposed a new optimal meeting location calculation algorithm which will also preserve the participants privacy.

.

ACKNOWLEDGEMENT

We would like to thank The Principal Dr. XYZ for providing him the opportunity to work on this project. We would like to show our sincere gratitude to our guide Prof. ABC for his guidance and idea without which this paper would not be complete. He provided us with important idea which helped me to accomplish writing this paper. I am also thankful to my HOD Prof. ABC Department of Computer Science, B.E for his constant encouragement and moral support..

REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu,"Digital Image Sharing by Diverse Image Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[2] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[3] K. H. Lee and P. L. Chiu, “Image size invariant visual cryptography for general access structures subject to display

quality constraints," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

[4] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[5] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.

[6] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for.