ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

An Obfuscation-Based Approach For Protecting Location Privacy

S.Thirunavukkarasu, Dr.K.P.Kaliyamurthie

Assistant Professor, Dept of IT, Bharath University, Chennai-73, India

Professor&Head, Dept of IT, Bharath University, Chennai-73, India

ABSTRACT: The pervasive diffusion of mobile communication devices and the technical improvements of location techniques are fostering the development of new applications that use the physical position of users to offer location-based services for business, social, or informational purposes. The concept of location privacy can be defined as the right of individuals to decide how, when, and for which purposes their location information can be released to other parties. The physical location of users is rapidly becoming easily available as a class of personal information that can be processed for providing new online and mobile services, generally called Location-Based Services (LBSs). Customer oriented applications, social networks, and monitoring services can be greatly enriched with data reporting where people are, how they are moving, or whether they are close to specific locations. In such a context, privacy concerns are increasing and call for sophisticated solutions able to guarantee different levels of location privacy to the users. In this project, we address this problem and present a solution based on different obfuscation operators that, when used individually or in combination, protect the privacy of the location information of users.

I.INTRODUCTION

The physical location of users is rapidly becoming easily available as a class of personal information that can be processed for providing new online and mobile services, generally called Location-Based Services (LBSs). In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. To protect location privacy, one typical approach is to apply different obfuscation operators used individually or in combination, protect the privacy of the location information of users.

II.PROJECT SCOPE

The concept of location privacy can be defined as the right of individuals to decide how, when, and for which purposes their location information can be released to other parties customer oriented applications, social networks, and monitoring services can be greatly enriched with data reporting where people are, how they are moving, or whether they are close to specific locations. In such a context, privacy concerns are increasing and call for sophisticated solutions able to guarantee different levels of location privacy to the users. In this paper, we address this problem and present a solution based on different obfuscation operators

III.OVERALL DESCRIPTION

Product Perspective

In our product, we address this problem and present a solution based on different obfuscation operators to protect the privacy of the location information of users. We also introduce an adversary model and provide an analysis of the proposed obfuscation operators to evaluate their robustness against adversaries aiming to reverse the obfuscation effects to retrieve a location that better approximates the location of the users. 1) we allow the users to express their privacy preferences in a simple and intuitive way and 2) to enforce the privacy preferences through a set of techniques robust against a relevant class of deobfuscation attacks

Product Features

Key aspects of our process, called obfuscation it means its allow users to express their privacy preferences in a simple and intuitive way and also enforce the privacy preferences through a set of techniques robust a against a relevant class of deobfuscation attacks while users have just to select a relevance value, the robustness of the solution is guaranteed by randomly selecting one of the techniques to produce the obfuscated location. We provide security to user information, by applying different obfuscation operators.

User Classes and Characteristics

Client - He is the person, who sends the query to the agent and receives the result
Agent - It acts as middleware, which receives and the send the query to the server, and send the result to the client
LBS - Location based server provides the result by processing the query.

Motivational Example

In order to motivate this project, consider the scenario illustrated in Figure 1.1.

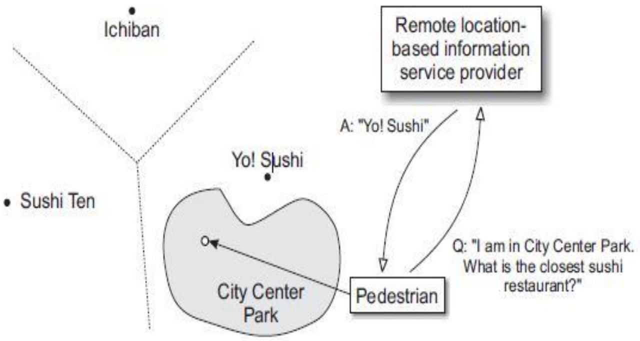
Ichiban
Remote location-based information service provider
A: "Yo! Sushi"
Yo! Sushi
Sushi Ten
O
City Center Park
Pedestrian
Q: "I am in City Center Park. What is the closest sushi restaurant?"

Fig. 1.1 An obfuscated location-based information service

A pedestrian wishes to access information about the address of the closest sushi restaurant, via a remote location-based service provider. Although there are three nearby restaurants, our hungry pedestrian would like to protect her privacy by providing only an approximate location to the information service provider. For example, the pedestrian can obfuscate her exact location by revealing only that she is in the "City Center Park." In this case, the service provider should still be able to correctly reply with the address of "Yo! Sushi," using basic spatial analysis algorithms (i.e., by constructing the Voronoi diagram for the sushi restaurants).

This example makes several simplifying assumptions, including a homogeneous Cartesian space with distance measured according to the Euclidean metric, and that the park does not overlap two proximal polygons. Nevertheless, this simple scenario does provide an intuitive example of a situation where it is possible to receive high-quality information services using low-quality positional information. It is this intuition that motivates this research.

Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

IV.PREVIOUS RESEARCH

In the existing system, the privacy of the users, which is already the centre of many concerns for the risks posed by current online services, can be threatened by LBSs. The publicity gained by recent security incidents that have targeted the privacy of users has revealed faulty data management practices and unauthorized trading of personal information (including ID thefts and unauthorized profiling). For instance, legal cases have been reported, where rental companies used the GPS technology to track their cars and charge users for agreement infringements, or where an organization used a location service to track its own employees. In addition, research on privacy issues has gained a relevant boost since providers of online and mobile services have often largely exceeded in collecting personal information in the name of service provision.

Current research on location privacy has mainly focused on supporting anonymity and partial identities. To a certain extent, anonymity and complete knowledge of personal information are the opposite endpoints of all the degrees of personal information knowledge managed by online services, and location information is just one type of personal information that often needs to be bound to a user identity. Anonymity is, however, not viable in the provision of an online service when the identification of users is required. In this case, a solution to protect the privacy of users consists in decreasing the accuracy of location information.

V.RESEARCH METHOD

In our system, we address this problem and present a solution based on different obfuscation operators to protect the privacy of the location information of users. We present a novel solution aimed at preserving the location privacy of the users by perturbing location information measured by sensing technologies. We focus on the development of techniques for protecting a single sample of location information. For the sake of concreteness, we consider locations gathered by means of cellular phones as our reference, even if our solution is not bound to a specific location technique. One important characteristic of cellular phones is their large availability and the possibility to be used as a source of location information both indoor and outdoor (on the contrary, GPS is operating mainly outdoor).

Key aspects of our perturbation process, called obfuscation, are:

To allow users to express their privacy preferences in a simple and intuitive way.

To enforce the privacy preferences through a set of techniques robust against a relevant class of deobfuscation attacks.

To this end, we introduce the concept of relevance as a metric of both location information accuracy and privacy that abstracts from the physical attributes of the sensing technology as well as from the actual technique employed to obfuscate a location. This way, while users have just to select a relevance value, the robustness of the solution is guaranteed by randomly selecting one of the techniques to produce the obfuscated location.

In this module, the client or the user can register with the system in order to use the location based service. The registration process includes filling up necessary details like full name, user name, password, age and email id. Once all the information are filled, the user is said to registered. After registration, the user can login the system with his user –name and password.

Now the user is allowed to use the location based service to see his current source location in Google maps. For this, under Map service, the user enters the address and the latitude – longitude value is fetched from internet. Saving this information, allows the user to view the source location of the user in Google maps.

We can find all the information related to the users, who ever have registered the system in our database. We can update the system, with all the location informations that we will be providing to the user.

The user now can search the required location information by sending a query which contains the details such as keyword, distance and privacy metrics. Keyword is what the user wants to search using the LSB. Distance is the distance range within which the user wants to search. Privacy metrics is nothing but privacy preference, which should be in the range 0 and 1. When the privacy metrics,

- tends to 0, when the location measurement is extremely inaccurate;

- is equal to 1, when the location measurement has achieved the best accuracy that the location techniques allow; and
- is in the range (0,1); otherwise, the higher the value, the higher the accuracy.

Obfuscation operators are applied to these values. The operators used here are Enlarge (E), Reduce (R) and Shift (S).These obfuscation operators are applied in the middleware, which convert the original location into a safe region and then it's sent to the service provided, where the given query is processed to provide information required by the user

The user now can search the required location information by sending a query which contains the details such as keyword, distance and privacy metrics. Keyword is what the user wants to search using the LSB. Distance is the distance range within which the user wants to search. Privacy metrics is nothing but privacy preference, which should be in the range 0 and 1. When the privacy metrics,

- tends to 0, when the location measurement is extremely inaccurate;
- is equal to 1, when the location measurement has achieved the best accuracy that the location techniques allow; and
- is in the range (0,1); otherwise, the higher the value, the higher the accuracy.

Obfuscation operators are applied to these values. The operators used here are Enlarge (E), Reduce (R) and Shift (S).These obfuscation operators are applied in the middleware, which convert the original location into a safe region and then it's sent to the service provided, where the given query is processed to provide information required by the user

VI. CONCLUSION

We presented different obfuscation operators that protect the location privacy of users by changing their location information. Our proposal takes into consideration both the accuracy of location measurements and the user's needs of privacy. We also provided an evaluation of the robustness of such operators. The analysis and the experimental results prove that our operators provide better protection than the simple enlargement usually applied by current solutions. Hence, we protect the location information of the user.

VII. FUTURE ENHANCEMENT

As future enhancement, the analysis of our solution assuming Gaussian-like distributions and complex location measurement shapes.

- the introduction of map constraints in the computation of obfuscated areas.
- the definition of additional techniques for degrading the temporal accuracy of location measurements.
- the extension of our solution to protect the path privacy of the users and
- the actual integration and extensive test of our solution in a real scenario.

REFERENCES

[1] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "Supporting Location-Based Conditions in Access Control Policies," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), Mar. 2006.

[2] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "A Middleware Architecture for Integrating Privacy Preferences and Location Accuracy," Proc. IFIP Int'l Information Security Conf. (SEC '07), May 2007.

[3] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and S. Samarati, "Location Privacy Protection through Obfuscation-Based Techniques," Proc. IFIP Working Conf. Data and Applications Security (DBSEC '07), July 2007.

[4] L. Barkhuus and A. Dey, "Location-Based Services for Mobile Telephony: A Study of User's Privacy Concerns," Proc. IFIP Int'l Conf. Human-Computer Interaction (INTERACT '03), Sept. 2003.

[5] P. Bellavista, A. Corradi, and C. Giannelli, "Efficiently Managing Location Information with Privacy Requirements in Wi-Fi Networks: A Middleware Approach," Proc. Int'l Symp. Wireless Comm. Systems (ISWCS '05), Sept. 2005.

[6] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.

[7] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in ocation-Aware Services," Proc. IEEE Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW '04), Mar. 2004.

[8] C. Bettini, X.S. Wang, and S. Jajodia, "Protecting Privacy against Location-Based Personal Identification," Proc. Second VLDB Workshop Secure Data Management, 2005.

[9] "Rental Firm Uses GPS in Speeding Fine," Chicago Tribune, p. 9, July 2001.

[10] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "K-Anonymity," Secure Data Management in Decentralized Systems, T. Yu and S. Jajodia, eds., Springer-Verlag, 2007.

[11] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Microdata Protection," Secure Data Management in Decentralized Systems, T. Yu and S. Jajodia, eds., Springer-Verlag, 2007.

[12] E. Damiani, M. Anisetti, and V. Bellandi, "Toward Exploiting Location-Based and Video Information in Negotiated Access Control Policies," Proc. Int'l Conf. Information Systems Security (ICISS '05), Dec. 2005.

[13] T. D'Roza and G. Bilchev, "An Overview of Location-Based Services," BT Technology J., vol. 21, no. 1, pp. 20-27, Jan. 2003.

[14] M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," Proc. Int'l Conf. Pervasive Computing (PERVASIVE '05), May 2005.

[15] M. Duckham and L. Kulik, "Dynamic & Mobile GIS: Investigating Change in Space and Time," Location Privacy and Location-Aware Computing, Taylor & Francis, 2006.