# Location Privacy In Android Smart Phone Using Obfuscation

**Jyotika P. Deshmukh**
**Department of Computer science and Engineering**
**G.H.Raisoni College of Engineering**
**Nagpur, India**

**S. U. Nimborkar**
**Department of Computer science and**
**G.H.Raisoni College of Engineering**
**Nagpur, India**

## ABSTRACT

**With advances in wireless communication and mobile positioning technologies, location-based services (LBSs) have been gaining increasingly popularity in recent years. On the other hand, the privacy threat of revealing a mobile user's personal information through his/her location has become a key issue to be concerned.users have made their locations more available than ever, representing a major privacy problem, as attackers could easily determine their victims' common paths or actual location**

**In this paper we study various techniques used for location protection and proposed the work which focuses on the development of techniques for protecting a location information from the adversary attack by using the obfuscation technique1) To allow users to state their private and public path and according to that provide privacy preferences in a simple and intuitive way . 2) To generate the obfuscation path which look similar to the original path.3) To protect the privacy of the users associated with location data, while maintaining an accuracy high enough to efficiently use location-based services**

## INTRODUCTION

THE rapid growth in mobile phones services make it possible to reveal the physical location of users and it is easily available as a class of personal information that can be processed for providing online and mobile services, 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. Several commercial and enterprise oriented LBSs are already available and have gained popularity (e.g., [4], [13], [16]), achieved in the field of sensing technologies. Location techniques allow to collect location information with good precision and reliability at costs that most people (e.g., the cost of current mobile devices like cellular phones) and companies (e.g., the cost of integrating location techniques in current telecommunication systems) can economically assist.

In this framework, the privacy of the users, which is already the center of many concerns for the risks posed by current online services [4], [9], [4], can be threatened by LBSs. The eye-opener 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 [9], or where an organization used a location service to track its own employees [5]. In addition, research on privacy issues has gained a significant boost since providers of online and mobile services have often largely exceeded in collecting personal information in the name of service provision.

In such a troublesome scenario, 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 improper exposure of location information could result in severe consequences that make users the target of deceptive attacks [15]. Current research on location privacy has mainly focused on supporting anonymity and partial identities [7], [8], [16], [19], [1]. 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 [2]. In this case, a solution to protect the privacy of users consists in decreasing the accuracy of location information [14], [3]. As a matter of fact, many LBSs do not need to have available location information as accurate as possible to offer an acceptable quality of service to users. In this paper we focus on the development of techniques for protecting a location information from the adversary attack by using the obfuscation technique. For the sake of concreteness, we consider locations gathered by means of cellular phones as our reference, 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 process, called obfuscation, are: 1) To allow users to state their private and public path and according to that provide privacy preferences in a simple and intuitive way and 2) To generate the obfuscation path which look similar to the original path.

The paper is organized as follows: Section II presents some related work in the area; Section III introduces the Matlock algorithm; Section IV shows the performance evaluation and finally, Section V presents the conclusions and future work.

**Location Privacy** is a particular type of data privacy. It is defined as the ability to prevent other unauthorized parties from learning ones' current or past location. In Location Based Services (LBSs), there are conceivably two types of location privacy: *personal subscriber level privacy* and *corporate enterprise-level privacy*. Personal subscriber-level privacy must supply rights and options to individuals to control when, why, and how their location is used by an application. With personal subscriber-level privacy, each individual has liberties to ``opt in" and ``opt out" of services that take advantage of their mobile location. Corporate enterprise-level privacy is fundamentally different in that corporate IT managers typically control when, why, and how mobile location capabilities provide application benefits to the organization as a whole. Within the enterprise, personal subscriber-level privacy is sometimes irrelevant because location is a critical requirement for staff to function productively while on the road. Asset tracking and workforce management are examples of location-enabled enterprise applications. However, companies need enterprise-level privacy to preserve corporate secrets and maintain competitive edge.

**Location Privacy Threats** refer to the risks that an adversary can obtain unauthorized access to raw location data, derived or computed location information by locating a transmitting device, hijacking the location transmission channel, and identifying the subject (person) using the device. For example, location information can be used to spam users with unwanted advertisements or to learn about users' medical conditions, alternative lifestyles or unpopular political views. Inferences can be drawn from visits to clinics, doctors' offices, entertainment districts, or political events. In extreme cases, public location information can lead to physical harm, for example, in stalking or domestic abuse scenarios [5,6].

Several approaches have been proposed for protecting location privacy of a user. Most of them try to prevent disclosure of unnecessary information by techniques that explicitly or implicitly control what information is given to whom and when. These techniques can be classified into three categories: (1) Location protection through user-defined or system supplied privacy policies [3,5]; (2) Location protection through anonymous usage of information, such as location cloaking, by reducing temporal and spatial resolutions of location information [1,2,3,6,7]; and (3) Location protection through pseudonymity of user identities, which uses an internal pseudonym rather than the user's actual identity [5]. Such pseudonyms should be different for different services and frequently changing to prevent applications tracking them. More importantly, such pseudonyms should be generated in such a manner that makes the linking between the old and the new pseudonym very hard [5].

**Location Privacy and Location Service Quality**

On one hand, the quality of the LBS depends on the accuracy of the location of mobile users, and on the other hand, the more accurate the location information is disclosed, the higher risk of location privacy is being invaded. There is an inherent tradeoff between the utility of a LBS that users wish to receive and the location privacy they can afford to risk. An important question is how much privacy protection is necessary.Perfect privacy is clearly impossible as long as communication takes place.

Moreover, different users may have varying privacy needs in different contexts. Furthermore, location privacy is context sensitive. Different users may require different levels of privacy at different times. A user's willingness to share location data may depend on a range of factors, including different contextual information about the user. Therefore, it is important to develop customizable/personalizedprivacy protection mechanisms that can help users finding a comfortable balance between the extreme of fully disclosed and completely withheld location data. This includes (i) the qualitative and quantitative analysis of the inherent tradeoff between the quality of service provided by the LBS and the desired location privacy of the user, (ii) how to determine and model the fuzziness of the location information sent by a mobile user to the LBS in order to reach such a tradeoff, and (iii) what types of user-defined privacy rules need to be combined with a personalized anonymization model to allow users to tailor the system-level privacy protection strategies to meet their personal privacy preferences.

**Location Anonymization** is a system capability to obfuscate the location information such that a state of a subject is not identifiable within the anonymity set.

Privacy and security have been active topics of research for the last few years, as there is a need to protect the location of users, who may be at risk from attackers looking for the exact information about the mobility patterns of the users. There are two main trends in location privacy: anonymity and obfuscation. The goal of anonymity is to prevent the traceability of location information.Some techniques use pseudonyms, third party location providers [3] or k-anonymity techniques in which a user’s exact location cannot be distinguishedamong k-1 other users [4], [5].Other anonymity techniques restrict access to the user’s locations, creating an “invisible cloaking” in which no location data is provided about geographical areas that are sensitive to the user, or which reduce resolution in time of the route [6].On the other hand, location obfuscation can be defined as “the means of deliberately degrading the quality of information about an individual’s location in order to protect that individual’s location privacy [7].” The main idea is for the original location to be altered, substituted, generalized or hidden in order to preserve the users privacy, while the LBS service provider still can provide a desirable level of service. Some of these techniques can be given parameters by the user in order to find a level of compromise of their location information in order to obtain better service. Many different location obfuscation techniques have been proposed. In [8], the authors generalize the location of the user by providing a broader area in which the user is, so that no actual location point is provided. In [9], the authors propose adding random noise to the data, or rounding the location based on a predefined set of landmarks or grid cells. Other schemes, use combined solutions including obfuscation and anonymity [10].There are some important disadvantages in these techniques. Firstly, they all reduce the accuracy of the location, so that it is almost impossible to recover the original point. Secondly, the distribution in time of the obfuscated points follows the same order as they were received, which provides a general idea of the trajectory taken. In Section III, a new approach will be proposed based on matrix obfuscation, which offers the possibility of transforming the space and time dimensions of the location information based on a small constant number of arithmetical operations. In addition, it is fully reversible so it can be used for applications where adding noise to the location has a negative impact on the service provided. To the knowledge of the authors, this is the first work that uses matrix obfuscation for location obfuscation.

## III Proposed Work

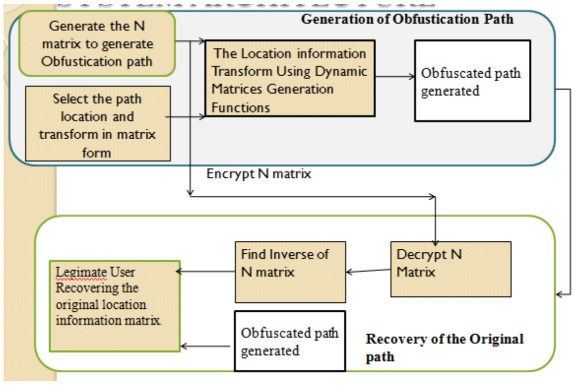
In the Existing system I find the attacker reversing the attacker reversing the obfuscated path presents a clear risk that attacker will have the exact location of the user without having to use any estimation algorithms. If the attackers already have 3 original locations of the user, they already may have enough critical information to follow the user in the real world and not through historic records in the system

The proposed system , is designed for the android operating system which is a light-weight and fully reversible location obfuscation technique .It requires low computation per operation and hides the location in both spatial and temporal dimension.This technique alters the location of paths from different geographical regions, produces a non-morphologically similar path to the original path.

As mentioned before, the main problem of traditional location obfuscation techniques is that they cannot alter the location information enough to avoid providing a coarse location of the user which could later be used to infer the actual location of the user. The approach described in uses a preliminary step in which the preferences of the users regarding the sensitive places and the desired degree of location privacy are collected. An obfuscation model is also proposed to model the user's preferences, based on the concepts of the properties of the place, the level of sensitivity, and the obfuscated space. The properties of the places are defined in order to specify if a place is sensitive (because the user doesn't want to reveal he is in it), unreachable (the user cannot be located in it), and non-sensitive otherwise. The level of sensitivity of a region is based on the extension and the nature of the sensitive places contained in it. For example, a region entirely filled with a hospital has a high level of sensitivity. The obfuscation method is then carried on in two steps: in the first step, the sensitive places specified by the user are obfuscated according to his preferences, generating a set of coarse locations instead of the actual locations. In the second step, when a user makes a location-based request, the obfuscation is enforced by mapping the position of the user onto an obfuscated position, generated in the first step.

## SYSTEM ARCHITECTURE

This work presents the Matlock algorithm, which uses N matrix obfuscation to transform the location points and their reception time considerably through a function with low computation complexity, and which is reversible in order to make recovery of the original location point and time possible. In addition, this technique can also add classical location obfuscation mechanisms in order to strengthen the security over the original location.Matrix obfuscation is a technique used to transform matrices in order to hide their content and the order in which they are located. One example of these techniques is the work of [12],in which the authors define a series of transforming operations that are used to later to define more complex transformation functions.In [13] the authors enumerate the basic operations involved in matrix transformation functions: scaling, addition, transpose, multiplication and inverse. one very important feature of the Matlock algorithm can be seen: the final obfuscated path presents no morphological similarities with the original one; in other words, the paths do not share general trends or shape similarities, despite the scale. This is one of the most important features that this technique offers because the transformation can be as severe as shaping a non-linear path into a linear route which gives little to no information that could be used for retracing the original route based on previously known locations from the user.


Generation of Obfustication Path
Generate the N matrix to generate Obfustication path
Select the path location and transform in matrix form
The Location information Transform Using Dynamic Matrices Generation Functions
Obfuscated path generated
Encrypt N matrix
Legimate User Recovering the original location information matrix
Find Inverse of N matrix
Decrypt N Matrix
Obfuscated path generated
Recovery of the Original path

## Matlock Algorithm:

Let M is the original Location of the user in form of Longitute Latitute and time

Let N be the matrix generated for each session

**1.Generation of Obfuscation pathat User side**

Whenever user used the Location based service the location of the user matrix M(1,3)=M(Longitude,Lattitude,Time)is generated

2.For each session new random matrix Generated N(3,3)

3.Combining the original matrix M with random matrix N generate the obfuscated path S=M X N.

N matrix is send to service provider in encrypted form

**Recovery of the original path at Service provider**

1.N matrix is decrypted

2.find the N inverse

3.Multiply the N -1 X S(1,3) matrix

## Conclusion

In the proposed work it provides right of the users to decide how, when, and for which purposes their location information can be released to other counterparts In this work we proposed the architecture for protecting the location privacy in the android phone by using the obfuscation technique using the Matlock Algorithm which is light weight and fully reversible

## REFERENCES:

[1] Xiao Pan, Jianliang Protecting Location Privacy against "Location-Dependent Attacks in Mobile Services" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 24, NO. 8, AUGUST 2012.

[2] Jie Liu, Xu Hu, Zhiqiang Wei, Dongning Jia, Chao Song “Location privacy protect model based on positioning middleware among the internet of things” 2012 International Conference on Computer Science and Electronics Engineering.

**[3]**Pedro M. Wightman, Miguel A. Jimeno, Daladier Jabba_ and Miguel Labradory **“**Matlock: A Location Obfuscation Technique for Accuracy-Restricted Applications**”** IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks 2012

[4] Chien-Ping Wu, Chen-Che Huang, and liun-Long Huang , Chib-Lin Hu “On Preserving Location Privacy in Mobile Environments” 978-1-61284-937-9 2011 IEEE .

[5]Li Ma Jiangchuan Liu Limin Sun Ouldooz Baghban Karimi “ “Trajectory Exposure Problem in Location-aware Mobile Networking 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems

**[6]** Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, and Pierangela Samarati” An Obfuscation-Based Approach for Protecting Location Privacy” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011

[7] Reza Shokri, George Theodorakopoulos, Carmela Troncoso ,Jean-Pierre Hubaux and Jean-Yves Le Boudec “Protecting Location Privacy:Optimal Strategy against Localization Attacks” CCS’12, October 16–18, 2012, Raleigh, North Carolina, USA. 2012 ACM 978-1-4503-1651

[8] W.G. Aref C.Y. Chow, M.F. Mokbel and G. Walid. “Casper*: Query processing for location services without compromising privacy”. ACM Transactions in Database Systems, 34:1–48, December 2009.

[9]H. Muller T. Rodden, A. Friday and A. Dix. A Lightweight Approach to Managing Privacy in Location-Based Services.Technical Report Equator-02-058. CSTR-07-006, University of Nottingham and Lancaster University and University of Bristol, 2002.

[10] M. Gruteser and D. Grunwald. “Anonymous usage of location-based services through spatial and temporal cloaking”. In Proceedings of MobiSys. LCNC 3468/2005, pages 31–42, 2003.

[11] Athens Trucks Data, http://www.rtreeportal.org/, 2006.

[12] ABI Researchhttp://www.abiresearch.com/press/1097-Mobile+Location+Based+Services+Revenue+to+Reach+$13.3+Billion+Worldwide+by+2013, 2008.

[13] O. Abul, F. Bonchi, and M. Nanni, “Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases,” Proc. IEEE 24th Int’l Conf. Data Eng. (ICDE ’08), pp. 376-385, Apr. 2008.

[14] B. Bamba and L. Liu, “Supporting Anonymous Location Queries in Mobile

Environments with Privacygrid," Proc. 17th Int'l Conf. World Wide Web (WWW '08), 2008.

[15] C. Bettini, X.S. Wang, and S. Jajodia, "Protecting Privacy against Location-Based Personal Identification," Proc. Second VLDB Workshop Secure Data Management, pp. 185-199, 2005.

[16] K. Bharath, G. Ghinita, and P. Kalnis, "Privacy-Preserving Publication of User Locations in the Proximity of Sensitive Sites,"
Proc. 20th Int'l Conf. Scientific and Statistical Database Management(SSDBM '08), July 2008.

[17] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," Proc. Privacy Enhancing Technology Workshop (PET '06),2006.

[18] C. Chow and M.F. Mokbel, "Enabling Private Continuous Queries for Revealed User Locations," Proc. 10th Int'l Conf. Advances inSpatial and Temporal Databases (SSTD '07), 2007.

[19] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, Official J. European Communities, pp. 37-47, 2002.

[20] J. Du, J. Xu, X. Tang, and H. Hu, "iPDA: Enabling Privacy-Preserving Location-Based Services," Proc. Conf. Mobile Data Management (MDM), 2007.

[21] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: Anonymous Location-Based Queries in Distributed Mobile Systems," Proc. 16th Int'l Conf. World Wide Web (WWW '07), 2007.

[22] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.

[23] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS '05), pp. 620-629, 2005.

[24] G. Ghinita, M.L. Damiani, and C. Silvestri, "Preventing Velocity- Based Linkage Attacks in Location-Aware Applications," Proc. 17th ACM SIGSPATIAL Int'l Conf. Advances in Geographic Information Systems (GIS '09), 2009.

[25] G. Gidofalvi, X. Huang, and T.B. Pedersen, "Privacy-preserving Data Mining on Moving Objects Trajectories," Proc. Int'l Conf.Mobile Data Management (MDM), 2007.