Poster: A Location-Privacy Approach for Continuous Queries

Doug Steiert
Department of Computer Science
Missouri University of Science and Technology
djsg38@mst.edu

Dan Lin
Department of Computer Science
Missouri University of Science and Technology
lindan@mst.edu

Quincy Conduff
Department of Computer Science
Missouri University of Science and Technology
qlcfz5@mst.edu

Wei Jiang
Department of Computer Science
Missouri University of Science and Technology
wjiang@mst.edu

ABSTRACT

With the prevalence of smartphones, mobile apps have become more and more popular. However, many mobile apps request location information of the user. If there is nothing in place for location privacy, these mobile app users are in great risk of being tracked by malicious parties. Although the location privacy problem has been studied extensively by resorting to a third-party location anonymizer, there is very little work that allows the users to fully control the disclosure of their data using their smartphones alone. In this paper, we propose a novel Android App called MoveWithMe which automatically generates mocking locations. Most importantly, these mocking locations are not random like those generated by original Android location mocking function. The proposed MoveWithMe app generates k traces of mocking locations and ensures that each trace looks like a trace of a real human and each trace is semantically different from the real user's trace.

ACM Reference format:
Doug Steiert, Dan Lin, Quincy Conduff, and Wei Jiang. 2017. Poster: A Location-Privacy Approach for Continuous Queries. In *Proceedings of SACMAT'17, Indianapolis, IN, USA, June 21-23, 2017,* 3 pages.
https://doi.org/http://dx.doi.org/10.1145/3078861.3084161

1 INTRODUCTION

Smartphones are a driving force in many actions that we do every day, and the number of smartphone owners has increased tremendously since their release. In correlation, the number of mobile phone applications have also exponentially risen alongside the growth of smartphone usage. A popular array of services that are combined with applications (apps) are known as Location Based Services (LBSs). While many users typically do not explicitly recognize these services being used, they are also unaware of the risks that are associated with them. In [1], Almuhimed et al. have conducted a field study on mobile app privacy and their findings show severe concerns on location privacy, e.g. someone's location has been shared 5,398 times with 10 apps within 14 days without being noticed by the user. Such loose control on location data by existing mobile apps has caused different types of privacy threats.

To mitigate risks to users' location-privacy, several strategies have been proposed. One typical approach is to add an access control mechanism to control the location disclosure to the selected service providers, such as the location privacy settings in iOS and Android systems. However, such access control does not prevent service providers which have been granted access permissions from tracking the users. In order to provide better privacy protection, some approaches [5] are proposed based on the spatial-temporal cloaking or k-anonymity. The basic idea is to let the user submit a bigger region instead of the exact location when requesting location-based services. Unfortunately, such strategies also have limitations. First, it trades-in the service quality since some types of services require accurate locations. For example, if a user would like to find nearby restaurants but tells the server his location at the city level, it would return all the restaurants in the city rather than just those near the user. There is a deeper issue in existing spatial-cloaking-based approaches, which is the lack of defense from attacks using aggregated information collected via continuous queries. For example, when someone uses an LBS constantly or frequently as he/she moves, the service provider may be able to narrow down possible places that the user visited and the user's moving direction.

In this research, we propose a novel location-privacy preservation app that is able to preserve smartphone users' location privacy. The main idea is to generate decoys that behave like real human movements and submit these decoys' locations to the service providers, along with the user's real locations. The goal is to prevent the service provider from profiling the real user. An overview of this approach is presented in Section 3.

2 RELATED WORK

Various approaches have been proposed to preserve location privacy, which can be classified into three main categories: (i) spatial-temporal cloaking based approaches; (ii) differential privacy based approaches; and (iii) encryption-based approaches.

The key idea of spatial-temporal cloaking is to generate a cloaking region that contains the user's real location and $k-1$ other users. In this way, the service provider would not be able to distinguish the k users in the same region and hence users achieve k-anonymity. The idea was first introduced by Gruteser et al. [7] and later has been extended by many [4, 14]. However, such approach suffers from the utility loss since users' queries would be based on the fuzzy

SACMAT'17, June 21-23, 2017, Indianapolis, IN, USA

ACM ISBN 978-1-4503-4702-0/17/06…$15.00
https://doi.org/http://dx.doi.org/10.1145/3078861.3084161

locations and would no longer be accurate. To achieve 100% query accuracy while cloaking the user's locations, Lin et al. [13] propose to use geo-transformation that converts user's real locations into a set of fake locations by multiple agents in-between the user and the server. The main limitation of the approach is that it only supports LBSs that query on moving objects but not any static objects like restaurants. More recently, Zang and Bolot [21] propose to publish shorter trajectories at a coarse granularity to prevent correlation of information obtained from call detail records with the users' true locations. However, such published trajectories will have little data utility.

The differential privacy based approaches add noise to the users' real data so that the providers would not know the true user locations. Andres et al. apply Laplacian noise to location data in a discrete Cartesian plane in [2]. Users are able to adjust the level of desired privacy, which increases the amount of noise added to the location. However, the downfall to this work is that the area of interest may not fall into the area once noise is added. The authors in [16] look at using k-anonymity to try to traverse the adversary's malicious attempts. By using dummy-location selection based on the entropy of locations, the user is more likely to be hidden. However, the region in which this location selection is performed might not be big enough to hide the user, especially if the adversary has background knowledge. Also, the proposed approach does not support continuous location-based queries. Differential privacy is also used in [15], in which Ngo and Kim reduce the average size of cloaking regions generated by the Hilbert curve. Chen et al. propose LISA in [3], which does not rely on a trusted third party for anonymization. LISA's core algorithm is based on unobservability along with a Kalman filter to adjust noise to location data. The limitation of LISA is that injecting noise to a location multiple times may lead the location to converge back to its original value. To sum up, a common limitation in all the differential privacy based approaches is that they trade in the service quality since they are not able to provide exact query results.

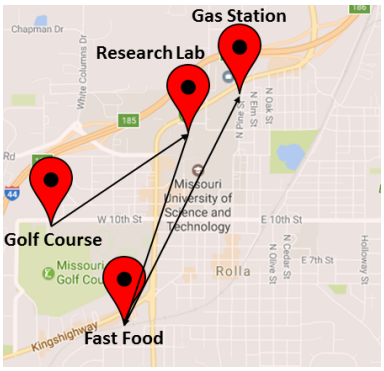
The encryption-based approaches aim to fully preserve the location privacy by encrypting the location data and conducting queries directly on the encrypted data. One representative work is by Ghinita et al. [6] who propose a framework to support private nearest neighbor queries based on Private Information Retrieval. In [12], Li and Jung devise a privacy-preserving location query protocol in which the locations of users are shared based on a condition-matching system. Location data is encrypted using Pallier encryption to ensure data security. Yet, this work requires an anonymized network which is currently unavailable for smartphones. Guha et al. [8] introduce a privacy-preserving framework which provides a cloud-based matching service to return attributes and their values in an encrypted fashion. Puttaswamy et al. [18] attempt to preserve location privacy in geo-social applications. Their work relies on the exchanging of secrets in order to encrypt/decrypt using 128-bit AES. However, they are oblivious to man-in-the-middle attacks during the exchange, and an adversary may easily discover those key values. Combining oblivious transfer and private information retrieval, Paulet et al. [17] aim to enable efficient processing of location queries. However, all the prior encryption-based approaches are typically too costly to be applied in practice.

Although there have been extensive studies on location privacy, very few have been devoted into developing mobile apps for users to control their locations. For example, in [9], Hornyack et al. implement a system which returns a fixed location and phone number at all times. While this can ensure privacy for the user, that user will never be able to enjoy most utilities of LBSs. Shokri et al. [19] devise a collaborative approach that allows peer users to form MobiCrowd. When a user needs to contact an LBS, his/her request will not be directly sent to the server but be routed through the MobiCrowd. In this way, the service provider will not know who sent the query. However, such strategy falls short when there are not enough users nearby. Most recently, Fawaz et al. [5] conducted a detailed risk analysis of the use of mobile apps in terms of location privacy leak. They propose an app called LP-Doctor which allows users to adjust the amount of location information to be disclosed to various apps. Compared to existing works, our proposed MoveWithMe is unique in the following aspects. First, it is not constrained by people density and can be used at any time. Second, it ensures the service quality in that the user is able to obtain the same query result. Third, it introduces very little overhead as evaluated in our experiments.

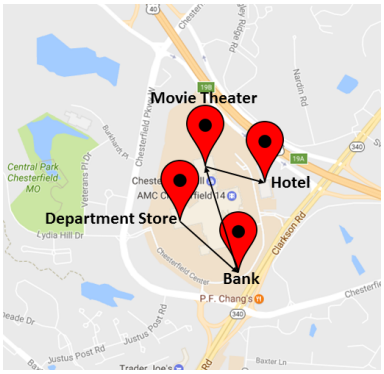
3 OUR PROPOSED ALGORITHM

Our proposed app is called MoveWithMe since it automatically generates a number of decoys to move with the user and serve as distractions to the service providers. Figure 1 shows an example use case, whereby Fig. 1(a) depicts the real user (say Bob)'s trajectory and Fig. 1(b) and (c) depict two decoys' trajectories. Specifically, assume that Bob wants to access a location-based service app (e.g., Yelp) when he is at the golf course at Rolla in the morning. As soon as Bob opens Yelp, the MoveWithMe will be activated and immediately generate two decoys, Decoy I and Decoy II as shown in the figure. Decoy I is visiting a department store in Chesterfield while Decoy II is in a physics class in a university in Columbia. The number of decoys can be set according to the user's privacy needs. By intercepting the user's interaction with Yelp, MoveWithMe will send the three locations to Yelp, as well. As time passes, Bob accessed the location-based services, when he went to his research lab and then to the fast food restaurant and the gas station. Meanwhile, one of its decoys would have visited a bank, a movie theater and a hotel, and the other decoy would have visited a pizza place, a hospital and a park. Observe that these three traces are not only located in different cities, but also demonstrate different social behaviors. In this way, it would be challenging for the service provider to identify the real user's trajectory and profile the real user without additional knowledge.

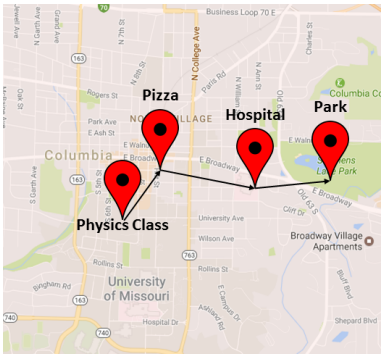
At the first look, our approach may seem to resemble the traditional use of dummy trajectories. However, our algorithms to generate dummy trajectories are fundamentally different. Traditional dummy trajectories [11, 16, 20] are geographically close to the real trajectory, and adversaries may still be able to discover the real user movement pattern using some pattern mining technique as reported in [10]. In our system, we are generating decoys which are not only geographically, but also semantically different from the real user's trajectory. Last but not the least, unlike the previous dummy trajectory works which are mostly developed at a theoretical level and rely on a central server, our system is more practical.



(a) Real User's Trajectory



(b) Decoy I's trajectory



(c) Decoy II's trajectory

Figure 1: An Example of Decoy Generation in the MoveWithMe App

The proposed MoveWithMe system is designed as an Android app that is capable of providing the privacy preservation for users at the real time.

ACKNOWLEDGMENTS

This work is supported by the National Science Foundation under Grant No: DGE-1433659.

REFERENCES

[1] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 787–796. ACM, 2015.

[2] Miguel E. Andrés, Nicolás E. Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 901–914, New York, NY, USA, 2013. ACM.

[3] Zhigang Chen, Xin Hu, Xiaoen Ju, and K. G. Shin. Lisa: Location information scrambler for privacy protection on smartphones. In *2013 IEEE Conference on Communications and Network Security (CNS)*, pages 296–304, Oct 2013.

[4] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar. Preserving user location privacy in mobile data management infrastructures. In *Proc. Workshop on Privacy Enhancing Technologies*, 2006.

[5] Kassem Fawaz, Huan Feng, and Kang G. Shin. Anatomization and protection of mobile apps' location privacy threats. In *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, pages 753–768, Berkeley, CA, USA, 2015. USENIX Association.

[6] Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and Kian-Lee Tan. Private queries in location based services: anonymizers are not necessary. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pages 121–132. ACM, 2008.

[7] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. MobiSys*, pages 31–42, 2003.

[8] Saikat Guha, Mudit Jain, and Venkata N. Padmanabhan. Koi: A location-privacy platform for smartphone apps. In *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*, NSDI'12, pages 14–14, Berkeley, CA, USA, 2012. USENIX Association.

[9] Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall. These aren't the droids you're looking for: Retrofitting android to protect data from imperious applications. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 639–652, 2011.

[10] Po-Ruey Lei, Wen-Chih Peng, Ing-Jiunn Su, and Chien-Ping Chang. Dummy-based schemes for protecting movement trajectories. *Journal of Information Science and Engineering*, 28(2):335–350, 2012.

[11] Po-Ruey Lei, Wen-Chih Peng, Ing-Jiunn Su, Chien-Ping Chang, et al. Dummy-based schemes for protecting movement trajectories. *Journal of Information Science and Engineering*, 28(2):335–350, 2012.

[12] X. Y. Li and T. Jung. Search me if you can: Privacy-preserving location query service. In *2013 Proceedings IEEE INFOCOM*, pages 2760–2768, April 2013.

[13] Dan Lin, Elisa Bertino, Reynold Cheng, and Sunil Prabhakar. Location privacy in moving-object environments. *Transactions on Data Privacy*, 2(1):21–46, 2009.

[14] M. F. Mokbel, C. Y. Chow, and W. G. Aref. The new casper: Query processing for location services without compromising privacy. In *Proc. VLDB*, pages 763–774, 2006.

[15] H. Ngo and J. Kim. Location privacy via differential private perturbation of cloaking area. In *2015 IEEE 28th Computer Security Foundations Symposium*, pages 63–74, July 2015.

[16] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li. Achieving k-anonymity in privacy-aware location-based services. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 754–762, April 2014.

[17] Russell Paulet, Md. Golam Koasar, Xun Yi, and Elisa Bertino. Privacy-preserving and content-protecting location based queries. In *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering*, ICDE '12, pages 44–53, Washington, DC, USA, 2012. IEEE Computer Society.

[18] Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao. Preserving location privacy in geosocial applications. *IEEE Transactions on Mobile Computing*, 13(1):159–173, January 2014.

[19] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J. P. Hubaux. Hiding in the mobile crowd: Locationprivacy through collaboration. *IEEE Transactions on Dependable and Secure Computing*, 11(3):266–279, May 2014.

[20] Tun-Hao You, Wen-Chih Peng, and Wang-Chien Lee. Protecting moving trajectories with dummies. In *8th International Conference on Mobile Data Management (MDM)*, pages 278–282, 2007.

[21] Hui Zang and Jean Bolot. Anonymization of location data does not work: A large-scale measurement study. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, MobiCom '11, pages 145–156, New York, NY, USA, 2011. ACM.