Using Dummy Locations to Conceal Whereabouts of Mobile Users in Location-Based Services

Sanjaikanth E Vadakkethil Somanathan Pillai (iD) https://orcid.org/0000-0003-3264-9923

School of Electrical Engineering and Computer Science, University of North Dakota, 243 Centennial Drive Stop 7165, Grand Forks, ND 58202-7165, USA

Wen-Chen Hu, (iD) https://orcid.org/0000-0003-3748-3280

School of Electrical Engineering and Computer Science, University of North Dakota, 243 Centennial Drive Stop 7165, Grand Forks, ND 58202-7165, USA

Abstract: Location-based services are extremely popular in these days. Mobile users use the services such as GPS and Google Maps almost every day to assist their daily activities like finding a restaurant or looking for an apartment. However, in order to use the services, users have to share their location information with the service providers. This requirement may hold back the service adaptation since users may not like to share their locations with others. One common method to preserve user privacy is to send a couple of dummy locations along with the true location to the service providers, so the provider would not be able to tell which location is true. This method is simple and effective, but it also has some drawbacks that make the privacy safeguarding fragile. If the dummy locations are not carefully planned, they may land on wild fields or water and could be easily perceived as fake. This research investigates the flaws of using dummy locations to uphold user privacy from both the users' and service providers' points of view, and proposes innovative methods to close the loopholes, so more users will be willing to use location-based services.

Keywords: Mobile computing, Security and privacy, Dummy locations, Location-based services, Smartphones

Introduction

Location-based services (LBSs), such as location-based advertising, mobile recommendations, and navigation, are very popular as the smartphones are used everywhere and anytime. However, in order to use the services, users have to share their location data with the service providers. Many users are reluctant to use the services because of this privacy concern. Various methods have been proposed to solve this problem. One of the methods, dummy locations, is used by many LBSs. It sends the true locations along with several fake locations to confuse the service providers, so the providers would not be able to tell the true one from the fake ones. The method is simple and effective, but the service providers may be able to figure out the true locations if the dummy locations are not generated carefully. For example, the 4 million miles of roads covered in the US is only a fraction of a percent of the total land area. If the dummy locations are not carefully planned, they may land on wild fields or water and could be easily perceived as fake.

Various loopholes from using the traditional methods of dummy locations are discussed first in this paper. Robust methods are then proposed to solve the problems. The following features must be taken into consideration when create dummy locations: (i) they should not be too far away from the true location, but cannot be too close to each other either, (ii) they should be located on the valid space like roads or parking lots, and (iii) their number should be kept as low as possible like 3 to 5. On the other end, the service providers will be able to tell the locations are fake if the above features are not followed. This research investigates the flaws of using dummy locations to uphold user privacy from both the users' and service providers' points of view, and proposes innovative methods to close the loopholes, so more users will be willing to use location-based services. Preliminary experiment results show the proposed method is simple, but effective.

The rest of this article is organized as follows. Section 2 gives the background information and related research of this research. Section 3 introduces the problems of current methods of dummy locations and Section 4 gives the proposed methods trying to solve the problems. Experiment results are shown in Section 5. The last section summarizes this research.

Background and Related Research

This section presents the related research of privacy-preserving methods for location-based services. Various methods of privacy preservation are discussed first and related dummy-location methods will be introduced next. An overview of dummy-based location privacy protection techniques for location-based services can be found from the article by Zhang, Li, Liang, Sandor, & Li (2022).

Privacy Preservation of Location-Based Services

Location-based services provide their services based on users' location information. Without proper privacy preservation, users would not like to use the services. They are many methods to preserve the users' privacy. This sub-section introduces some of the methods. One of the methods is spatial cloaking, which obscures a user's true location into a cloaked area, so there is low possibility of associating users to locations. Pan, Meng, & Xu (2009) propose a δ_p-privacy model and a δ_q-distortion model to balance the tradeoff between user privacy and QoS (quality of service).

Furthermore, two incremental utility-based cloaking algorithms—bottom-up cloaking and hybrid cloaking, are proposed to anonymize continuous queries. Montazeri, Houmansadr, and Pishro-Nik (2016) use a method of anonymization (identity perturbation instead of location perturbation) to achieve location privacy. A random permutation $\Pi^{(N)}$ is applied to the set of N users, and then the pseudonym $\Pi^{(N)}(i)$ is assigned to the user i. They claim perfect privacy can be achieved under certain conditions by using their method. Wang, Hu, Sun, & Huang (2018) propose a query content preservation approach with the aim of providing accurate LBS answer with zero server knowledge on query content. Peng, Liu, Wang, Xiang, & Chen (2019) propose a multidimensional privacy preservation scheme that provides full protection for user privacy without any need for a trusted third

party. The proposed scheme employs a semi-trusted middle entity to perform user anonymization and result-blind filtering while unaware of any sensitive information regarding the mobile users. They utilize the Hilbert curve to transform user locations, and preserve users' query contents using encryption technology. Related research can be found in the articles (Chow & Mokbel, 2011b; Deutsch, Hull, Vyas, & Zhao, 2010; Wu, Wang, Li, Lian, Xu, Chen, & Liu, 2020) and surveys of privacy-preserving techniques for location-based services are given in the articles (Chow, Mokbel, & Liu, 2011; Jiang, Li, Zhao, Zeng, Xiao, & Iyengar, 2021) or a book (Chow & Mokbel, 2011a).

Privacy Preservation Using Discrete Dummy Locations

For dummy/fake locations, users send their true location data along with several dummy/false location data to the service providers. User location privacy is preserved because service providers cannot distinguish the true location data from the dummies. Though this approach is effective, it is also simple, so not many articles put the focus on this approach. Zhang & Li (2022) preserve the user privacy by using the following three steps. First, the dummy location candidate set is constructed based on WordNet by randomly selecting offset location, and conforming to probability similarity. The dummy location set is then filtered out by discretizing dummy locations based on the Heron formula. Finally, the secure anonymity set is constructed according to the anonymity level. Sun, et al. (2019) propose a region-of-interest division-based algorithm to preserve the location privacy of mobile device users in location-based services.

Unlike existing methods, the proposed approach generates dummy locations while considering the semantic information of those locations. It enables the generated locations to exclude or reduce the exposure of a user's real location. Pingley, Zhang, Fu, Choi, Subramaniam, & Zhao (2011) develop a user-centric technique for query privacy protection which operates solely on the user side and does not require any trusted third party. The key idea is to confuse the adversary by issuing multiple counterfeit queries with varying service attributes but the same (real) location, henceforth referred to as dummy queries, along with each real query issued by the user. Wang and Xie (2018) propose a scalable location privacy preservation (LPP) method based on the paradigm of counterfeiting locations by forging the fake locations through synthesizing artificial impostors (AIs). Two dedicated techniques are devised: the sampling-based synthesis method and population-level semantic model. Bindschaedler and Shokri (2016) design a privacy-preserving generative model to synthesize location traces. The location traces are plausible to be trajectories of some individuals with consistent lifestyles and meaningful mobility. Related research can also be found in the articles (Lu, Jensen, & Liu, 2008; Yao, Lin, Liu, Deng, & Wu, 2012).

Privacy Preservation Using Continuous Dummy Locations

Other than creating discrete dummy locations to preserve privacy, location-based services may consider generating continuous dummy locations for hiding the traveling trajectories. Sun, Ma, Song, Yue, Lin, & Ma (2022) use three real-life trajectory datasets, five existing anonymization mechanisms (identifier anonymization, grid-based anonymization, dummy trajectories, k-anonymity and ε-differential privacy), and two practical

applications (travel time estimation and window range queries) to faciltate privacy preservation for continuous location-based services. They found there is a long way to go for the privacy preservation for trajectories in the general sense. An attack model representing a realistic privacy threat on user trajectories is proposed by Shaham, Ding, Liu, Dang, Lin, & Li, (2020). They also propose a metric called transition entropy that enables the evaluation of dummy-based algorithms, followed by developing a robust algorithm that can defend users against the attack while maintaining significantly high performance in terms of the traditional metrics. Zhang, Qian, Ding, Ma, Li, & Shaham (2019) propose an algorithm based on the k-anonymity criterion, to generate dummy locations to protect users' privacy. Their simulation results on the real-life dataset show the proposed algorithm performs better than other methods. Related articles can be found from the articles (Huang, Xu, Chen, & Xie, 2022; *Zhang, Wang, Bhuiyan, & Liu, 2018*)

Problems of Using Dummy Locations

Location-based services (LBSs) require the users to report their information such as user IDs, location data, time stamps, landmarks, etc. The LBS users are assumed to receive the recommendations immediately after they send their information to the service providers, which supply the recommendations upon request. This section discusses various methods for creating dummy locations and their associated problems.

Discrete Dummy Locations

Location-based services (LBSs) require the users to report their information such as user IDs, location data, time stamps, landmarks, etc. The LBS users are assumed to receive the recommendations immediately after they send their information to the service providers, which supply the recommendations upon request. This section discusses various methods for creating dummy locations and their associated problems. For simple location-based services, like finding a nearby ethnic restaurant based on the user's current location, the user's privacy may be revealed if the dummy locations are not generated carefully. Two kinds of dummy locations are generally used in this approach, random locations within a distance and random locations, and are discussed next.

- *Random locations within a distance*: Random locations are randomly generated within a distance d from the true location. For example, Figure 1 shows four dummy locations, *D1-D4* and the true location, *T1*. It seems the service provider would not know which location is true. Therefore, it will generate five sets of recommendations based on the five locations, respectively. However, if the service provider is smart enough, it may figure out an approximate distance $d' \leq d$ after few rounds. The longest distance l, like *|D1-D2|*, is collected in each round. After a while, the d' would be the longest one l' of the collected distances divided by 2 like $d'=l'/2$. Once the approximate distance d' is found, some dummy locations could be eliminated. For example, *D1* could not be a true location because each of the distances *|D1-D2|* and *|D1-D3|* is much greater than d'. For the same reason, *D2* could not be the true location, either. Therefore, the true location may be one of the three locations, *T1*, *D3*, and *D4*.
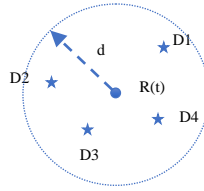
Figure 1. Four Dummy Locations (*D*) Generated Based on the True Location (*R*) at the Time *t*

- *Random locations*: Dummy locations are generated randomly. Figure 2 shows four dummy locations (*D*) randomly generated. After several rounds of generations, some locations may be ruled out as the true location (*T*). For example, the *D1* may be dropped if no previous locations can reach it according to the distance based on time stamps and calculated travel speeds.
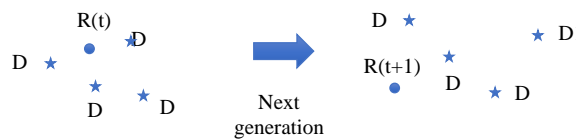

Figure 2. True Location (*R*) and Four Dummy Locations (*D*) Generated Randomly at the Times *t* and *t+1*

Continuous Dummy Locations

Continuous LBSs require users to continuously send their location data to service providers. For example, better transportation planning is based on traffic flows instead of vehicle counts; recommendations (like interesting places) would be more effective if travel routes (sequences of locations), not individual locations, are used. Compared to LBSs, continuous LBSs have more pitfalls. The following list shows the problems may be caused by continuous LBSs:

- *Random locations within a distance*: The two endpoints of a dummy route are random locations within a distance *d* from the true locations. Figure 3 shows an example of this approach. The major problem of this approach is the service provider may pick one route and treat it as the true route. The result may not be much different because the true route is close to dummy routes, so an approximate true route may be found. Another problem of this approach is the end point of a segment is the start point of the next segment. The service provider may be able to figure out the true route after receiving few segments because the dummy routes all are surrounding the true route.
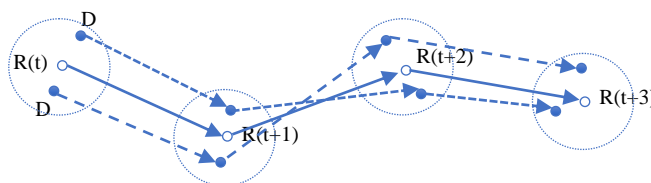

Figure 3. Dummy Routes Created by Using Random Locations (*R*) within a Distance from the True Location *R* at Different Times (*t*)

- *Random locations*: The dummy routes are generated randomly. Figure 4 shows an example of this approach. The problem of this approach is the dummy routes may be far away from the true route after a while and maintain and keep track of them may not be easy. If the dummy routes are not planned carefully, the service provider may figure out the true route. For example, if the dummy locations could not be reached in a specific time according to the previous locations, road and street conditions, and the travel speeds, then they may be ruled out as true routes.
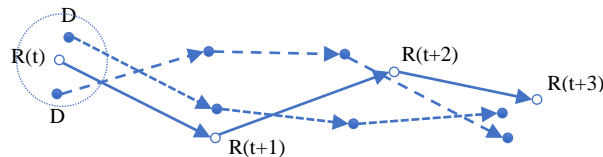

Figure 4. Dummy Routes Created by Using Random Locations (*D*)

The Proposed Methods

This research proposes genuine dummy location generation, so the service providers will not be able to tell which the true locations are. This research proposes a robust dummy locations and routes to solve the problems mentioned in the previous section. The methods are also discussed according to LBSs and continuous LBSs. Compared to LBSs, continuous LBSs are more challenging because the users have to continuously report their location data to the service providers and it makes their privacy more fragile.

Discrete Location-Based Services

The problem of dummy locations discussed in the previous section is some dummy locations may be ruled out because the distance *d* may be figured out, where random locations are randomly generated within a distance *d* from the true location. Instead of building the system from the ground up, this research tries to solve the problem by generating genuine dummy locations based on Roads API of Google Maps Platform (Google, n.d.), which identifies the roads a vehicle was traveling along and provides additional metadata about those roads, such as speed limits. The proposed algorithm is given as follows:

1. Find the device location including latitude and longitude.
2. Generates three random locations (latitudes and longitudes) within a distance from the device location.
3. The new latitude is a random double value that is between the integer-converted device latitude and the next integer such as

   lat = integer (device latitude)

   new latitude = float [lat, lat+1]
4. Find the longitude by using a similar formula as above.

5. Call Google Maps API for Road (https://roads.googleapis.com/v1/nearestRoads) by passing the three pairs of latitudes and longitudes delimited by the symbol '|', for example,

    https://roads.googleapis.com/v1/nearestRoads?points=34.5082,-97.6989|34.51352,-97.7397|34.52352,-97.7197

6. The returned three locations (latitudes and longitudes) are on a road within 50-60 meters to the input latitude and longitude. If there is no such road found, it will return null.

Continuous Location-Based Services

Instead of sending the location data to the service providers constantly, this research has the users send their routes (sequences of locations) to the service providers. There are several advantages of using this approach. First, the performance is higher because the location data does not need to be sent frequently. Another advantage is the privacy preservation is better as discussed in this section. However, compared to dummy locations, dummy routes are more difficult to build since roads and streets have to be considered. For example, if a portion of the routes crosses a building, the route may be fake. Instead of building the dummy routes from the ground up, this research takes the advantage of Google Direction API (Application Programming Interface), which is a service that calculates directions between locations using an HTTP request. Users can search for directions for several modes of transportation, include transit, driving, walking or cycling. Directions may specify origins, destinations and waypoints either as text strings (e.g. "Chicago, IL" or "Darwin, NT, Australia") or as latitude/longitude coordinates. The proposed methods are discussed according to how the locations are generated. The dummy routes are generated randomly. Figure 5 shows an example of this approach. The problem of this approach is the dummy routes may be far away from the true route after a while and maintain and keep track of them may not be easy. If the dummy routes are not planned carefully, the service provider may figure out the true route. For example, if the dummy route is very long or crosses a building, then it may be ruled out as a true route. The problem of dummy routes discussed in the previous section is either dummy routes are too close to the true route or it is difficult to maintain the dummy routes. Hu, Kaabouch, & Yang (2016) give the proposed algorithm of dummy-location generation for location-based services:

1. Generate *n* dummy locations randomly based on the true locations, *R* and *R1*, respectively.
2. Generate *n+1* routes by using Google Direction API based on the true and dummy locations.
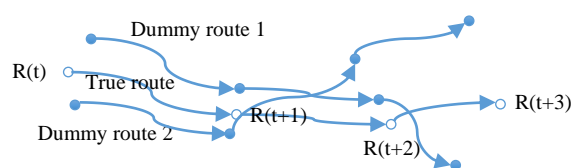3. Send the true and dummy routes to the server.

Figure 5. Dummy Routes Created by Using Random Locations

Experiment Results

This section is to show the results of our method by building a prototype system, which is to recommend the mobile user an interesting place based on the user quests and location. In order to receive the recommendation, the user has to send his/her current location information to the service provider. Instead of actual road testing, this experiment uses Android emulators to perform the testing. Actual road testing will be conducted in the future.

Experiment Setup

This sub-section discusses a prototype of a location-based service for showing the effectiveness of the proposed method. The proposed service is made simple on purpose and its system structure is shown in Figure 6, where a set of services are saved by the service provider before the app is put to use. When the user requests a recommendation, his/her current location along with three dummy locations are sent to the service providers. The recommended destinations are sent back to the user and a route between the current location and the genuine destination is drawn. The proposed system can be found from GitHub (E Vadakkethil Somanathan Pillai, 2022).
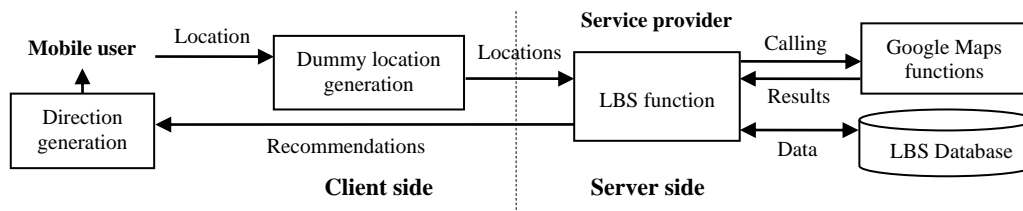

Figure 6. System Structure of the Proposed Location-Based Service

The LBS Database is a tiny geographical database including three tables: *Events*, *Transactions*, and *Sequences*, whose schema and sample values are given in Figure 7 (Hu, Kaabouch, & Yang, 2016). The *Events* table stores a small set of events such as restaurants, motels, and entertainment events like theaters and concerts. Each transaction or sequence consists of a list of events. The difference between a transaction and a sequence is the events of the former are unordered, whereas the ones of the latter are ordered. In addition, each item of a sequence is an event, instead of a set of events.

Events			
EID	**Type**	**Name**	**Location**
E01	Restaurant	Gourmet Café	47° 55' 31" N, 97° 01' 57" W
E02	Motel	Best Motel	47° 55' 37" N, 97° 01' 63" W
E03	Theater	AMC	47° 55' 28" N, 97° 01' 59" W
E04	Restaurant	Pasta House	47° 55' 38" N, 97° 01' 84" W
...	...	...	...

Transactions	
T#	**EID**
T05	E12
T02	E03
T05	E26
T24	E18
...	...

Sequences		
S#	**EID**	**Next**
S01	E03	S04
S02	E12	S10
S03	E38	S54
S01	E27	—
...	...	...

Figure 7. Schemas and Sample Values of the Tables *Events*, *Transactions*, and *Sequences*

The Result Screenshots

This sub-section shows some of the screenshots from this service. It is to help readers understand what the service can achieve. Instead of doing actual road tests, this research uses Android AVD (Android Virtual Device) to simulate the testing. Figure 8 shows three screenshots from this app. Figure 8.a shows the app in the Android Launcher, Figure 8.b is the control panel associated with the emulator, and Figure 8.c is the extended controls after clicking the item at the bottom of the control panel. The extended controls include a location function, which allows users to enter location data including latitude, longitude, and attitude and submit it to the app. Using this function is similar to the app receiving location data from the GPS (Global Positioning System).
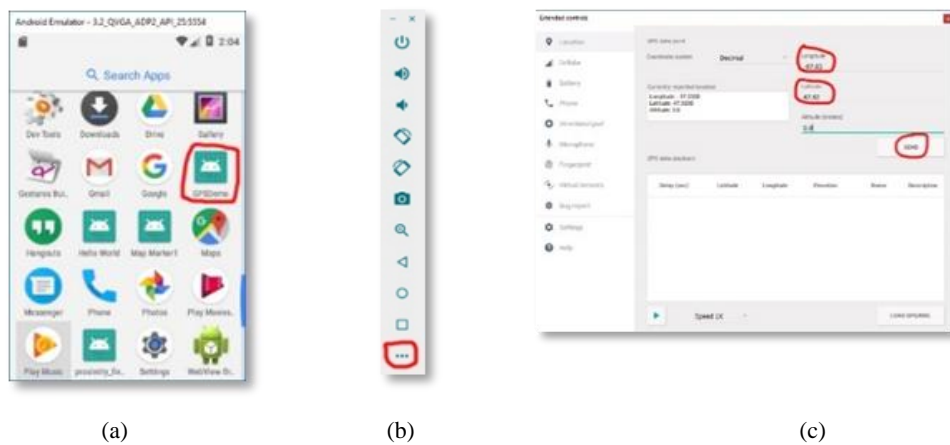

(a) (b) (c)

Figure 8. (a) The Proposed App Shown in the Android Launcher, (b) the Control Panel, and (c) the Extended Controls

Figure 9 shows dummy locations generated by the proposed method. All locations are valid as they are not located at improper locations like water, buildings, or wild fields.
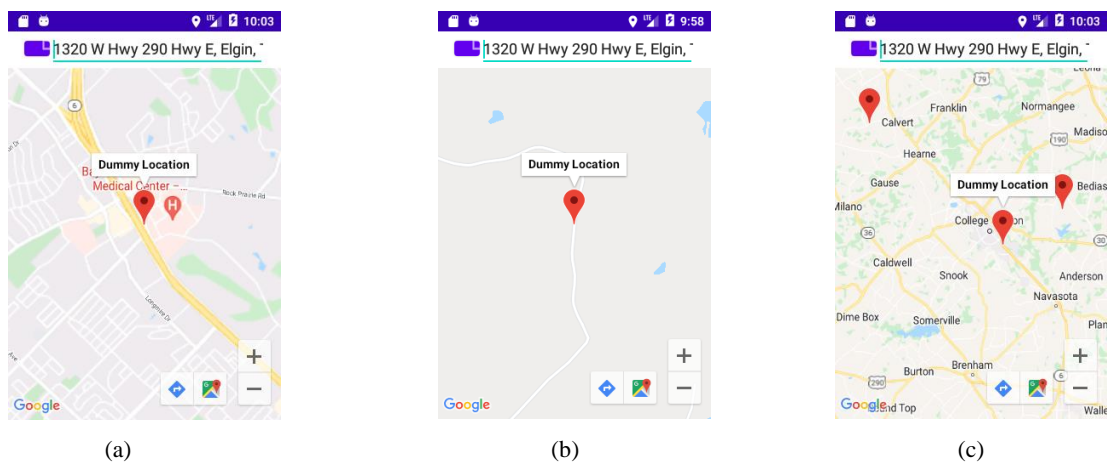

(a) (b) (c)

Figure 9. Valid Dummy Locations Generated by the Proposed Method

Figure 10.a shows the user is marked according to his/her current location sent from the extended controls of Android. Figure 10.b shows three valid dummy locations are generated by our method in addition to the user true location, and a direction between the user and a recommended destination is drawn in Figure 10.c by using Google Maps Direction API.
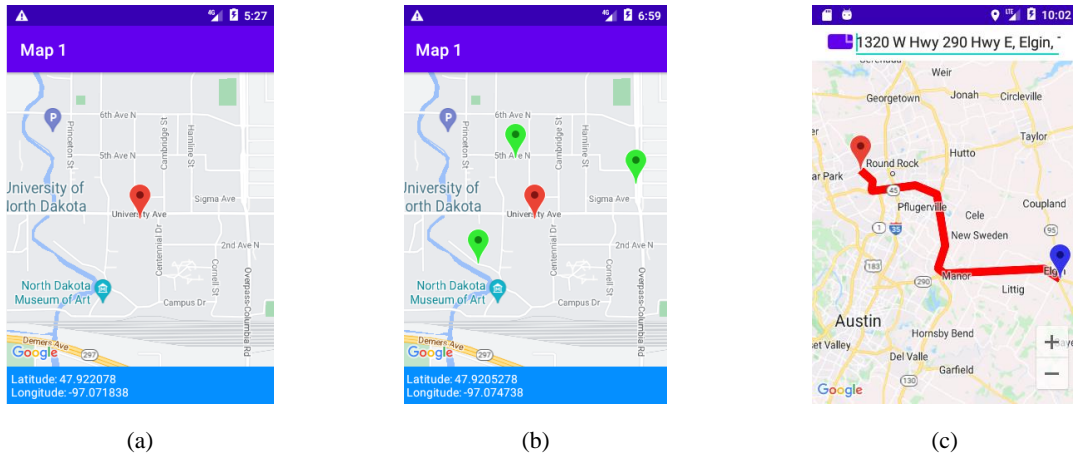

Figure 10. (a) User Location Marked, (b) Three Dummy Locations Generated, and (c) Direction Between the User and a Recommended Destination

Examples of dummy routes are given in Figure 11, where (a) shows two locations. Figure 11.b displays a direction generated by using Google Maps Direction API. A dummy direction based on the true direction is shown in the Figure 11.c.

Figure 11. (a) Two Locations Marked, (b) a Direction Drawn, (c) a Dummy Direction Created

Conclusion

Smartphones are extremely popular in these days. People carry them everywhere and use them anytime. Smartphones include many features such as high mobility, low bandwidth, and small screens not found in desk or lap-top computers. Because of their unique features, new usage data of smartphones is generated and new

research and applications are created. One of the applications, location-based services (LBSs), is to provide services based on user locations. However, there is one major concern for these services: user privacy preservation. Most LBSs require the users' current locations and many users are reluctant to share their locations and identities. Dummy (fake) locations have been used frequently in location-based services to protect users' privacy. Users send their true location data along with dummy location data to the service providers. User privacy is assumed to be preserved because service providers cannot distinguish the true location data from the dummies'. This approach is simple and seems effective. However, it is not without problems because user privacy may not be protected if it is not planned carefully.

The service providers may be able to figure out the true locations if the dummy locations are not generated carefully. For example, the 4 million miles of roads covered in the US is only a fraction of a percent of the total land area in the lower 48 states. The dummy locations may land on wild fields or water and could be easily perceived as fake. This research first shows the possible pitfalls of the method of dummy locations. A robust method is then proposed to solve the problems. In addition, most LBSs use not only discrete locations, but also continuous locations. This research also considers sending continuous dummy locations to service providers and upholding the user privacy. Preliminary experiment results show this method is simple and effective for privacy preservation of location-based services. However, actual road testing and solid proofs need to be given to prove the effectiveness and robustness of the proposed method. The ideas will be further improved or revised based on users' feedbacks and testing data.

References

Bindschaedler, V. & Shokri, R. (2016, May 23-25). Synthesizing plausible privacy-preserving location traces. In *Proceedings of the IEEE Symposium on Security and Privacy* (*S&P 2016*), San Jose, California.

Chow, C.-F., Mokbel, M. F., & Liu, X. (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *Geoinformatica*, *15*, 351-380.

Chow, C.-Y. & Mokbel, M. F. (2011a). Privacy of spatial trajectories. In Y. Zheng and X. Zhou (Eds.), *Computing with Spatial Trajectories* (pp. 109-141). New York: Springer.

Chow, C.-Y. & Mokbel, M. F. (2011b). Trajectory privacy in location-based services and data publication. *SIGKDD Explorations*, *13*(1), 19-29.

Deutsch, A. Hull, R., Vyas, A., & Zhao, K. K. (2010, March 1-6). Policy aware sender anonymity in location based services. In *Proceedings of the 26th International Conference Data Engineering* (*ICDE 2010*), Long Beach, California, USA.

E Vadakkethil Somanathan Pillai, S. (2022). Google Maps with privacy preservation. Retrieved from https://github.com/sanjaikanth/GooleMapWithPrivacy

Google. (n.d.). Roads API of Google Maps Platform. Retrieved from https://developers.google.com/maps/documentation/roads/overview

Hu, W.-C., Kaabouch, N., & Guo, H. (2019, July 6-9). Location privacy protection using dummy locations and routes. In *Proceedings of the 23rd World Multi-Conference on Systemics, Cybernetics and Informatics* (*WMSCI 2019*), *Orlando, Florida, USA*.

Hu, W.-C., Kaabouch, N., & Yang, H.-J. (2016, May 19-21). Secure spatial trajectory prediction based on traffic flows. In *Proceedings of the 2016 IEEE International Electro/Information Technology Conference* (*EIT 2016*), Grand Forks, North Dakota, USA.

Huang, Q., Xu, X., Chen, H., & Xie, L. (2022). A vehicle trajectory privacy preservation method based on caching and dummy locations in the internet of vehicles. *Sensors*, *22*, 4423. 10.3390/s22124423.

Jiang, H., Li, J., Zhao, P., Zeng, F., Xiao, Z., & Iyengar, A. (2021). Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys* (*CSUR*), *54*(1), 1-36.

Lu, H., Jensen, C. S., & Liu, M. L. (2008, June 13). PAD: Privacy-area aware, dummy-based location privacy in mobile devices. In *Proceedings of the 7th ACM International Workshop on Data Engineering for Wireless and Mobile Access* (*Mobide 2008*), Vancouver, British Columbia, Canada.

Montazeri, Z., Houmansadr, A., & Pishro-Nik, H. (2016, March 16). Defining perfect location privacy using anonymization. In *Proceedings of the 2016 Annual Conference on Information Science and Systems* (*CISS 2016*), pages 204-209, Princeton, New Jersey, USA.

Pan, X., Meng, X., & Xu, J. (2009, November 4-6). Distortion-based anonymity for continuous queries in location-based mobile services. In *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems* (*ACM SIGSPATIAL GIS 2009*), pages 256-265, Seattle, Washington, USA.

Peng, T., Liu, Q., Wang, G., Xiang, Y., & Chen, S. (2019). Multidimensional privacy preservation in location-based services. *Future Generation Computer Systems*, *93*, 312-326.

Pingley, A., Zhang, N., Fu, X., Choi, H.-A., Subramaniam, S., & Zhao, W. (2011). Protection of query privacy for continuous location based services. In *Proceedings of the 30th IEEE International Conference on Computer Communications* (*INFOCOM 2011*), pages 1710-1718, Shanghai, China.

Shaham, S., Ding, M., Liu, B., Dang, S., Lin, Z., & Li, J. (2020). Privacy preservation in location-based services: A novel metric and attack model. *IEEE Transactions on Mobile Computing*, *20*(10), 3006-3019.

Sun, G., Cai, S., Yu, H., Maharjan, S., Chang, V., Du, X., & Guizani, M. (2019). Location privacy preservation for mobile users in location-based services. *IEEE Access*, *7*, 87425-87438, https://doi.org/10.1109/ACCESS.2019.2925571.

Sun, S., Ma, S., Song, J.-H., Yue, W.-H., Lin, X.-L., & Ma, T. (2022, September 30). Experiments and Analyses of anonymization mechanisms for trajectory data publishing. *Journal of Computer Science and Technology, 37*, 1026–1048, https://doi.org/10.1007/s11390-022-2409-x

Wang, C. & Xie, Z. (2018). Artificial impostors for location privacy preservation. *arXiv:1801.06827 [cs.SI]*.

Wang, S., Hu, Q., Sun, Y., & Huang, J. (2018). Privacy preservation in location-based services. *IEEE Communications Magazine*, *56*(3), 134-140.

Wu, Z., Wang, R., Li, Q., Lian, X., Xu, G., Chen, E., & Liu, X. (2020). A location privacy-preserving system based on query range cover-up or location-based services. *IEEE Transactions on Vehicular Technology*, *69*(5), 5244-5254.

Yao, L., Lin, C., Liu, G., Deng, F., & Wu, G. (2012, August 20-24). Location anonymity based on fake queries in continuous location-based services. In *Proceedings of the 2012 7th International Conference on Availability, Reliability and Security* (*ARES 2012*), pages 375-382, Washington, DC.

Zhang, A. & Li, X. (2022). Research on privacy protection of dummy location interference for location-based service location. *International Journal of Distributed Sensor Networks*, *18*(9), https://doi.org/10.1177/15501329221125111

Zhang, L., Qian, Y., Ding, M., Ma, C., Li, J., & Shaham, S. (2019). Location privacy preservation based on continuous queries for location-based services. In *Proceedings of IEEE INFOCOM 2019–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1-6.

Zhang, S., Li, M., Liang, W., Sandor, V.K.A., & Li, X. (2022). A survey of dummy-based location privacy protection techniques for location-based services. *Sensors*, *22*:6141, https://doi.org/10.3390/s22166141

Zhang, S., Wang, G., Bhuiyan, M., & Liu, Q. (2018). A dual privacy preserving scheme in continuous location-based services. *IEEE Internet of Things Journal*, *5*, 4191-4200.