1. Introduction

1.1. Overview of the Anonymity

Recently, the dependency of the smartphone devices applications on location has been dominating the Google Play and Apple stores [1]. Therefore, Location-Based Services (LBSs) are becoming essential in everyone's lifestyle. Furthermore, for example, in Uber/Uber-like applications [2], the user must reveal his/her location to request private drivers. Moreover, the need of the location information is not limited to the location-based applications, but the location information is also used in some social network applications such as Facebook [3] and Twitter [4]. Facebook uses the location information to let the user know about nearby friends [5], while Twitter uses the location to find tweets posted by people nearby [6].

Although disclosing the personal location enables many applications to provide user-tailored services, however, on the other hand, this practice might threat the user's privacy. For example, when an adversary can acquire the location of a certain user and he/she can use this information for tracking the user or identify the regular locations of the user visits. Therefore, location privacy is a crucial issue in mobile applications and social networks.

One of the existing approaches that are proposed to handle the location privacy issue is the k-anonymity scheme [7]. The k-anonymity scheme hides the individual's location by using a set of $k-1$ other locations. There are many schemes that use the k-anonymity to preserve the location privacy such as Dummy Location Selection (DLS) scheme and Enhanced Dummy Location Selection (EDLS) scheme [7]. Both schemes hide the real location of the user by using a set of dummy locations. The process of selecting the dummy locations in both schemes are based on k-anonymity.

1.2. Research Objectives

This thesis deals with $\boldsymbol{k}$-anonymity to protect the location privacy. The major goal and objectives of this thesis are summarized as follows.

- Introducing a novel scheme, namely, User-Based Location Selection (UBLS) using $\boldsymbol{k}$-anonymity. The UBLS scheme takes into consideration the user's query probability, which is different from the existing schemes such as DLS [7], Moving in a Neighborhood (MN) [8]. It chooses $\boldsymbol{k-1}$ dummy users whose query probabilities are close to the query probability of

the requester (i.e., the user who requests a service from the LBSs server), then it uses the $k-1$ dummy users' locations to hide the location of the requester.

- Proposing an Attacker Location Exclusion (ALE) algorithm that can be used to attack many existing privacy-preserving schemes that do not take into consideration users' query probabilities. The ALE attempts to find the location of the requester among other $k-1$ locations by excluding the locations that have low probabilities to be the requester's location. We use the ALE algorithm against the UBLS scheme and other existing schemes such as DLS [7], MN [8] to show which scheme is better in preserving location privacy when the LBSs server is malicious.
- Proposing a new metric denominated as a Location Privacy Level (LPL), and it qualifies the ability of the malicious LBSs server to reduce the privacy level of the requester.
- Evaluating the proposed UBLS scheme and compare it with different benchmarks schemes [7], [8].

1.3. Research Methodology

The methodology that is used in the novel algorithm in this thesis (UBLS scheme) is based on k-anonymity concept. The general idea of the proposed algorithm is an improvement of the DLS algorithm [7]. Instead of using dummy locations to anonymize the user's location as in the DLS algorithm, the proposed algorithm restricts the dummies to the users' locations whose query probabilities are close to the query probability of the target user. The proposed algorithm consists of two phases. In the first phase, the target user enters her/his query probability and her/his location. In the second phase, the proposed algorithm performs certain computations to select the dummy locations based on the query probabilities of other users. Also, the methodology takes into consideration the performance metrics that measure the anonymity level of the proposed algorithm and other related schemes. This thesis focuses on the well-known performance metrics which are entropy and cloaking region metrics in addition to the proposed metric (LPL metric).

1.4. Summary

This chapter gave an overview for the basic topic of the thesis which is preserving the location privacy of the user. Then the main objectives of the thesis were given. Moreover, the methodology was presented in this chapter.

References

[1] W. Martin, F. Sarro, Y. Jia, Y. Zhang, and M. Harman, “A Survey of App Store Analysis for Software Engineering,” *IEEE Trans. Softw. Eng.*, vol. 43, no. 9, pp. 817–847, 2017.

[2] T. Kalanick and G. Camp, “Uber - Earn Money by Driving or Get a Ride Now,” *Uber.com*, 2018. https://www.uber.com/ (accessed Dec. 15, 2018).

[3] M. Zuckerberg, E. Saverin, A. McCollum, D. Moskovitz, and C. Hughes, “Facebook,” *Facebook*, 2018. https://www.facebook.com/ (accessed Dec. 15, 2018).

[4] J. Dorsey, N. Glass, E. Williams, and B. Stone, “Twitter,” *Twitter.com*, 2018. https://twitter.com/ (accessed Dec. 15, 2018).

[5] Y. Lin, C. Lai, J. William Chapman, S. Felix Wu, and G. Barnett, “Geo-Location Identification of Facebook Pages,” in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Barcelona, Spain, 2018, pp. 441–446.

[6] G. Abalı, E. Karaarslan, A. Hürriyetoğlu, and F. Dalkılıç, “Detecting citizen problems and their locations using twitter data,” in *6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, Istanbul, Turkey, 2018, pp. 30–33.

[7] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, “Achieving k-anonymity in Privacy-Aware Location-Based Services,” presented at the IEEE Conference on Computer Communications, 2014, pp. 754–762.

[8] H. Kido, Y. Yanagisawa, and T. Satoh, “An anonymous communication technique using dummies for location-based services,” in *Proceedings of International Conference on Pervasive Services*, 2005.