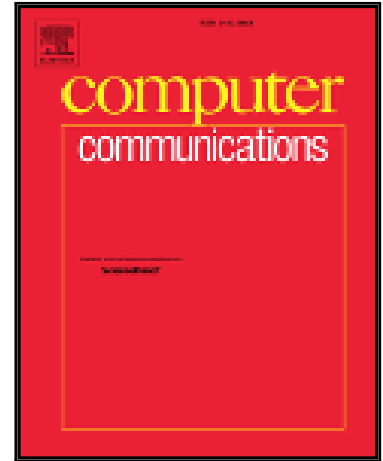


Accepted Manuscript

Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks

Mahdi Daghmehchi Firoozjaei, Jaegwan Yu, Hyoungkee Choi, Hyoungshick Kim

PII: S0140-3664(16)30345-0
DOI: [10.1016/j.comcom.2016.09.008](https://doi.org/10.1016/j.comcom.2016.09.008)
Reference: COMCOM 5384



To appear in: *Computer Communications*

Received date: 17 December 2015
Revised date: 19 July 2016
Accepted date: 17 September 2016

Please cite this article as: Mahdi Daghmehchi Firoozjaei, Jaegwan Yu, Hyoungkee Choi, Hyoungshick Kim, Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks, *Computer Communications* (2016), doi: [10.1016/j.comcom.2016.09.008](https://doi.org/10.1016/j.comcom.2016.09.008)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks

Mahdi Daghmehchi Firoozjaei¹, Jaegwan Yu¹, Hyoungkee Choi¹,
Hyoungshick Kim^{1,*}

Abstract

Although location-based services (LBSes), such as nearest neighbor query, have become popular, privacy remains a challenging issue for users. Many privacy preserving techniques have been proposed, but their complexity, insufficiency, and time consumption make them unattractive to users, who prefer accuracy and quickness. To address this limitation, we introduce a framework to protect user privacy for nearest neighbor queries by utilizing the basic geographical features of cellular networks. In the proposed framework, we provide two layers of spatial anonymity such that the user's location is not directly provided to a location service provider. Based on the features of the cellular network (e.g., LTE) at the first layer, the user's location is kept hidden under the cloaking of the base station (eNB) that provides a network connectivity to serve the user (SeNB). At the second layer, we anonymize SeNB in a group of dummy locations neighboring a central eNB (CeNB), all of which have the same query probability. Unlike most existing approaches with faked dummy locations, the proposed framework depends on real locations of eNBs to minimize the likelihood that side information might be exposed to an adversary. Moreover, our model is motivated by the practicality of employing the ubiquity of cellular networks and their geographical features. The simulation results show that the proposed scheme can achieve a decent degree of accuracy (> 98%) while providing strong privacy guaran-

*Corresponding author

Email addresses: mdaghmechi@skku.edu (Mahdi Daghmehchi Firoozjaei),
jaegwan@skku.edu (Jaegwan Yu), meosery@skku.edu (Hyoungkee Choi),
hyoung@skku.edu (Hyoungshick Kim)

¹College of Information & Communication Engineering, Sungkyunkwan University, Suwon, Republic of Korea

Download English Version:

<https://daneshyari.com/en/article/4954480>

Download Persian Version:

<https://daneshyari.com/article/4954480>

[Daneshyari.com](https://daneshyari.com)