UNIVERSITY OF TECHNOLOGY SYDNEY
Faculty of Engineering and Information Technology

Location Privacy Protection in Social Networks

by

Mohammad Reza Nosouhi

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Sydney, Australia

2020

Certificate of Authorship/Originality

I, Mohammad Reza Nosouhi declare that this thesis, is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Computer Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Mohammad Reza Nosouhi

Production Note:
Signature removed prior to publication.

Date: 22/07/2020

Acknowledgements

I would like to express my gratitude to my primary supervisor, Professor Shui Yu, who guided me throughout this research. I appreciate all the time he has spent on editing my papers, discussing my research ideas, and listening to my problems. It was a great privilege and honor to work and study under his guidance.

I would also like to give my sincere thanks to Dr Marthie Grobler, my supervisor in CSIRO's DATA61 who spent a lot of time on editing my papers and constantly provided me with advice, help and support.

It is my fortune to gratefully acknowledge the personal and professional support of my friend and research collaborator, Dr Keshav Sood. I aquired a lot of skills and experiences from him during my PhD study.

I wish to acknowledge the financial support provided by an Australian Government Research Training Program Scholarship (RTPS) and also a CSIRO's Data61 Top–Up scholarship. This work would not have been possible without their support. I would also like to express my appreciation to all the staff members of Faculty of Engineering and Information Technology and also UTS library, whose services turned my research a success.

Finally, yet importantly, I would like to thank my parents for their love and support throughout my life. Most importantly, I wish to thank my loving and supportive wife, Neda, who provided endless support and inspiration. Without her encouragement and understanding, this thesis wouldn't exist.

Mohammad Reza Nosouhi

Sydney, Australia, 2020.

List of Publications

Journal Papers

J-1. MR. Nosouhi, K. Sood, S. Yu, M. Grobler, "PASPORT: A Secure and Private Location Proof Generation and Verification Framework", *IEEE Transactions on Computational Social Systems*, vol. 7, Issue 2, pp. 293–307, Apr 2020. Available online at: `https://ieeexplore.ieee.org/document/8967030`

J-2. MR. Nosouhi, S. Yu, W. Zhou, and M. Grobler, "Blockchain for Secure Location Verification", *Journal of Parallel and Distributed Computing*, vol. 136, pp. 40–51, Feb 2020. Available online at: `https://www.sciencedirect.com/science/article/abs/pii/S074373151930320X`

J-3 L. Cui, Y. Qu, MR Nosouhi, S. Yu, J.W. Niu, and G. Xie, "Improving Data Utility Through Game Theory in Personalized Differential Privacy", *Journal of Computer Science and Technology*, vol.34, pp. 272–286, 2019. Available online at: `http://jcst.ict.ac.cn/EN/10.1007/s11390-019-1910-3`

Conference Papers

C-1. MR. Nosouhi, S. Yu, K. Sood, and M. Grobler, "HSDC–net: Secure Anonymous Messaging in Online Social Networks", *IEEE TrustCom*, 2019. Available online at: `https://ieeexplore.ieee.org/document/8887315`

C-2. MR. Nosouhi, S. Yu, M. Grobler, Y. Xiang, and Z. Zhu, "SPARSE: Privacy–Aware and Collusion Resistant Location Proof Generation and Verification", *IEEE GLOBECOM*, 2018. Available online at: `https://ieeexplore.ieee.org/document/8647933`

C-3. MR. Nosouhi, Y. Qu, S. Yu, Y. Xiang, and D. Manuel, "Distance –Based Location Privacy Protection in Social Networks", *International Telecommu-*

nications Network and Applications Conference, 2017. Available online at: https://ieeexplore.ieee.org/document/8215390

C-4. MR. Nosouhi, V. H. Pham, S. Yu, Y. Xiang, and M. Warren, "A Hybrid Location Privacy Protection Scheme in Big Data Environment", *IEEE GLOBECOM*, 2017. Available online at: https://ieeexplore.ieee.org/document/8254987

Contents

List of Figures

List of Tables

ABSTRACT

Location Privacy Protection in Social Networks

by

Mohammad Reza Nosouhi

Social networks have become more ubiquitous due to new advances in smartphone technology. This has provided an opportunity for social network service providers to utilise location information of users in their services. For example, Facebook Places, Foursquare and Yelp are popular social networks that mostly rely on utilising users' location data in their services. They offer a variety of useful services, from location recommendations to nearby friend alerts. However, protecting location privacy of users is still an open challenge for social network service providers. It has been shown that hiding real identity and choosing a pseudonym does not guarantee to protect a user's privacy since privacy may be invaded by analysing position data only. This is really a big issue since other private information of users can be revealed by analysing their location data (e.g., home address, health condition, interests, etc.).

In this study, we investigate the location privacy issue of social networks and propose several solutions. We classify the proposed solutions into three categories based on the selected approaches, i.e. (i) differential privacy-based, (ii) cryptography-based, and (iii) anonymity-based solutions. We first study the approach in which differential privacy is utilised to preserve privacy of users. In this regard, we develop Distance–Based Location Privacy Protection mechanism (DBLP2), a customisable location privacy protection approach that is uniquely designed for social network

users. It utilises the concept of social distance to generalise users' location data before it is published in a social network. The level of generalisation is decided based on the social distance between users.

Secondly, we study cryptography-based methods for location privacy protection in Location–Based Services (LBS) and social networks. In this domain, we propose three cryptography-based and privacy–aware location verification schemes to preserve location privacy of users: (i) Privacy–Aware and Secure Proof Of pRoximiTy (PASPORT), (ii) Secure, Privacy–Aware and collusion Resistant poSition vErification (SPARSE), and (iii) a blockchain–based location verification scheme. These schemes prevent location spoofing attacks conducted by dishonest users while protect location privacy of users. To the best of our knowledge, majority of the existing location verification schemes do not preserve location privacy of users.

Thirdly, we investigate anonymity as another approach to preserve users' privacy in social networks. In this regard, we first study the relevant protocols and discuss their features and drawbacks. Then, we introduce Harmonized and Stable DC–net (HSDC–net), a self–organizing protocol for anonymous communications in social networks. As far as we know, social networks do not offer any secure anonymous communication service. In social networks, privacy of users is preserved using pseudonymity, i.e., users select a pseudonym for their communications instead of their real identity. However, it has been shown that pseudonymity does not always result in anonymity (perfect privacy) if users' activities in social media are linkable. This makes users' privacy vulnerable to deanonymization attacks. Thus, by employing a secure anonymous communication service, social network service providers will be able to effectively preserve users' privacy.

We perform extensive experiments and provide comprehensive security and privacy analysis to evaluate performance of the proposed schemes and mechanisms.

Regarding the DBLP2 mechanism, our extensive analysis shows that it offers the optimum data utility regarding the trade–off between privacy protection and data utility. In addition, our experimental results indicate that DBLP2 is capable of offering variable location privacy protection and resilience to post processing. For the SPARSE scheme, our analysis and experiments show that SPARSE provides privacy protection as well as security properties for users including integrity, unforgeability and non–transferability of the location proofs. Moreover, it achieves a highly reliable performance against collusions. To validate performance of the PASPORT scheme, we implement a prototype of the proposed scheme on the Android platform. Extensive experiments indicate that the proposed method can efficiently protect location–based applications against fake submissions. For the proposed blockchain–based scheme, our prototype implementation on the Android platform shows that the proposed scheme outperforms other currently deployed location proof schemes. Finally, our prototype implementation of the HSDC–net protocol shows that it achieves low latencies that makes it a practical protocol.

In summary, this research study focuses on developing new mechanisms for preserving location privacy of social network users. This is done through different approaches. Moreover, extensive effort is made to make the current location–related schemes and protocols privacy–aware. In this regard, several solutions in the form of scheme, mechanism, and protocol are introduced and their performance is evaluated. The results of this research work have also been presented in seven papers published in peer-revewied journals and conferences.

Keywords: anonymous communications; customizable differential privacy; data privacy; DC–net; location privacy; location–based services; location proof; social distance; social networks.