

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 GLOBE-COM*, 2017. Available online at: <https://ieeexplore.ieee.org/document/8254987>

Contents

Certificate	ii
Acknowledgments	iii
List of Publications	iv
List of Figures	xi
List of Tables	xv
Abstract	1
Chapter 1: Introduction	4
1.1 Background	4
1.2 Problem Statement	7
1.3 Research Questions	8
1.4 Research Objectives	9
1.5 Scientific Contributions	10
1.6 Thesis Organization	12
1.7 Conclusion	13
Part I Differential Privacy–Based Approach	15
<hr/>	
Chapter 2: Literature Review and Preliminaries	16
2.1 Introduction	16
2.2 Literature Review	17
2.3 Preliminaries	21

2.3.1	Differential Privacy	22
2.3.2	Laplace Mechanism	23
2.4	Conclusion	24
Chapter 3: Customisable Location Privacy Protection in Social Networks		25
3.1	Introduction	25
3.2	Background	26
3.3	The Proposed DBLP2 Mechanism	28
3.3.1	System Architecture	29
3.3.2	Graph Model	30
3.3.3	Converting Social Distances to Privacy Levels	32
3.3.4	Customisable Differential Privacy	34
3.4	Conclusion	37
Chapter 4: Results		39
4.1	Introduction	39
4.2	System Analysis	39
4.3	Performance Evaluation	44
4.4	Conclusion	49
Part II Cryptography–Based Approach		50
<hr/>		
Chapter 5: Literature Review and Preliminaries		51
5.1	Introduction	51
5.2	Literature Review	52
5.2.1	Centralized Schemes	52

5.2.2	Distributed Schemes	53
5.3	Preliminaries	56
5.3.1	Blockchain Overview	63
5.3.2	Design Challenges:	64
5.4	Conclusion	68
Chapter 6: PASPORT: Secure and Private Location Proof		
Generation and Verification		70
6.1	Introduction	70
6.2	Background	72
6.3	PASPORT: The Proposed Scheme	75
6.3.1	Architecture and Entities	75
6.3.2	Trust and Threat Model	76
6.3.3	P-TREAD	77
6.3.4	The Workflow of PASPORT Framework	80
6.3.5	Witness Trust Model	84
6.3.6	PASPORT Usability	86
6.4	Results	87
6.4.1	Security and Privacy Analysis	87
6.4.2	Performance Evaluation	94
6.5	Conclusion	98
Chapter 7: SPARSE: Privacy-Aware and Collusion Resistant		
Location Proof Generation and Verification		99
7.1	Introduction	99
7.2	The SPARSE Scheme	100
7.3	Results	104

7.3.1	Security and Privacy Analysis	104
7.3.2	Performance Evaluation	107
7.4	Conclusion	109
Chapter 8:	Blockchain for Secure Location Verification	111
8.1	Introduction	111
8.2	The Proposed Architecture	112
8.3	Results	119
8.3.1	Security and Privacy Analysis	119
8.3.2	Implementation Results	124
8.4	Conclusion	127
Part III	Anonymity–Based Approach	128
<hr/>		
Chapter 9:	Literature Review and Preliminaries	129
9.1	Introduction	129
9.2	Literature Review	130
9.3	Preliminaries	134
9.3.1	DC–net Overview	134
9.3.2	DC–net Drawbacks	136
9.3.3	The Short Stability Issue	137
9.4	Conclusion	138
Chapter 10:	Anonymity in Social Networks	139
10.1	Introduction	139
10.2	HSDC–net: Secure Anonymous Messaging in Online Social Networks .	140
10.2.1	Protocol Description	140

10.3 Results	146
10.3.1 Security Analysis	147
10.3.2 Performance Evaluation	148
10.4 Conclusion	152
Chapter 11: A Hybrid Location Privacy Protection Scheme in Big Data Environment	154
11.1 Introduction	154
11.2 Background	155
11.3 Assumptions and Definitions	157
11.3.1 User’s Location Privacy Requirement	158
11.3.2 Analysis of a Correlation–Aware Scheme	159
11.4 The Hybrid Scheme	160
11.4.1 Direction Filter	161
11.4.2 Time Reachability Filter	162
11.4.3 Detached/Hub Filter	162
11.5 Analysis on the proposed scheme	163
11.6 Performance Evaluation	164
11.6.1 Evaluation Setup	164
11.6.2 Results	165
11.7 Conclusion	167
Chapter 12: Summary	168
12.1 Introduction	168
12.2 Conclusion	168
Chapter : Bibliography	171

List of Figures

1.1	Research Objectives	10
2.1	Methods for location privacy protection in location-based services	19
3.1	The proposed DBLP2 system architecture.	29
3.2	A simple example showing three users of a social network modelled by a simple graph.	31
3.3	An example of four users with different privacy protection requirements.	33
4.1	Probability density function for generalised gamma distribution.	41
4.2	The magnitude of the injected noise for a (A) conservative user, (B) very relaxed user, (C) relaxed user, and (D) moderate user.	45
4.3	The result of a collusion attack in which five users with different social distances from the victim have shared their response to obtain a more accurate location data.	47
5.1	Distance-bounding protocols are generally exposed to three types of security attacks: (a) Distance Fraud, (b) Mafia Fraud, and (c) Terrorist Fraud.	58
5.2	Message exchange diagram for TREAD	60
5.3	An example of P-P collusions.	65

6.1	The proposed system architecture.	76
6.2	Message flow between the three entities of the proposed scheme.	80
6.3	Success probability of a Prover–Witness collusion for different values of K_D and system parameters.	92
6.4	(a) CPU usage for different key sizes. (b) and (c) Time required for LP generation in our scheme, STAMP [25], and APPLAUS [26] under different key sizes. In APPLAUS, the authors have not implemented their scheme for key sizes larger than 256.	94
6.5	(a) and (b) Time required for LP generation over different physical distances. The shown measurements are for the key sizes 2048 for (a) and 256 for (b). (c) P–TREAD distance bounding protocol takes most of the time required for LP generation.	95
6.6	Outdoor path for the mobility tests (300 meters).	97
6.7	Time required for LP generation when multiple witness devices are involved. (a) outdoor and (b) indoor environments.	98
7.1	The system architecture of SPARSE Scheme	100
7.2	Message exchange diagram for the proposed scheme.	101
7.3	The success probability of Prover–Witness collusions. (A) $\beta = 40\%$ (B) $\beta = 60\%$ and (C) $\beta = 80\%$	108
7.4	The average number of colluding witnesses that are selected by the verifier for (A) $K = 8$ (B) $K = 10$ and (C) $K = 12$	109
8.1	Message exchange diagram of the proposed scheme	113
8.2	In the proposed scheme, each transaction can have different inputs and outputs.	113
8.3	Block creation and transaction structure in the proposed scheme.	114

8.4	(a) CPU usage for different key sizes. (b) and (c) Time required for LP generation in our scheme, STAMP, and APPLAUS under different key sizes. (d) and (e) Time required for LP generation over different physical distances. (f) Time required for Tx generation after a witness receives message m_3	125
8.5	The percentage of LP requests that successfully pass the P-P collusion detection test for different values of T	126
9.1	The Dining Cryptographers network in a simple example.	135
10.1	HSDC-net system architecture.	140
10.2	A simple illustration of SR performance.	143
10.3	Probability of collision after a single run of SR for (a) $B = 3$ and (b) $B = 5$	149
10.4	(a) Time required to initialize the protocol, reserve a slot, and perform one cycle of anonymous message publishing. (b) End-to-end latency to publish an anonymous post.	150
10.5	Time required to reserve B slots in a single run of SR for different values of B	151
10.6	End-to-end latency to anonymously publish a tweet for HSDC-net and some well-known anonymity schemes.	152
11.1	The concept of Spatiotemporal correlation issue between 2 neighbouring location sets.	157
11.2	Our proposed system architecture. Unlike K-Anonymity methods, there is no need to have a trusted third-party anonymizer.	159
11.3	An example of two neighbour location sets at time T_{i-1} and T_i	159
11.4	Average number of indistinguishable movement paths for 1.5K initial candidate dummies.	166

11.5 Average number of indistinguishable movement paths for 3K initial
candidate dummies. 166

List of Tables

1.1	List of Contributions	11
5.1	Comparison of LP Schemes	54
5.2	Comparison of the success probability of different security threats for some well-known DB protocols	59
5.3	List of Cryptographic Notations	61
7.1	List of Notations	102
11.1	Summary of Notation	158
11.2	The Average number of dummy regenerations for different numbers of initial candidate dummies	165

ABSTRACT

Location Privacy Protection in Social Networks

by

Mohammad Reza Nosouhi

Social networks have become more ubiquitous due to new advances in smart-phone 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 PASSPORT 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-reviewed journals and conferences.

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