UNIVERSIDADE D
COIMBRA

Mariana da Cruz Cunha

PRIVACY-PRESERVING MECHANISMS FOR LOCATION TRACES

Dissertation in the context of the Master in Informatics Engineering, Specialization in Software Engineering, advised by Professor João Paulo da Silva Machado Garcia Vilela and presented to Faculty of Sciences and Technology / Department of Informatics Engineering.

July 2019

This page is intentionally left blank.

Faculty of Sciences and Technology

Department of Informatics Engineering

Privacy-Preserving Mechanisms for Location Traces

Final Report

Mariana da Cruz Cunha

Dissertation in the context of the Master in Informatics Engineering, Specialization in Software Engineering, advised by Professor João Paulo da Silva Machado Garcia Vilela and presented to the Faculty of Sciences and Technology / Department of Informatics Engineering.

July 2019

UNIVERSIDADE D
COIMBRA

This page is intentionally left blank.

Acknowledgements

To my advisor, Professor João Paulo da Silva Machado Garcia Vilela, for the total availability, for all the support and guidance throughout the development of this thesis

To my "co-advisor", Ricardo da Silva Mendes, for all the advices and the recommendations.

To my family, especially, to my parents and to my sister, for the motivation and the support during my life.

To all those who somehow were present and contributed to completing this stage of my journey.

This work is supported through projects SWING2 (PTDC/EEI-TEL/3684/2014) and Mobiwise (P2020 SAICTPAC/001/2015), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização - COMPETE 2020 and by National Funds from FCT - Fundação para a Ciência e a Tecnologia, through project POCI-01-0145-FEDER-016753, and European Union's ERDF (European Regional Development Fund).

This page is intentionally left blank.

Agradecimentos

Ao meu orientador, Professor João Paulo da Silva Machado Garcia Vilela, pela total disponibilidade, por todo o apoio e orientação ao longo do desenvolvimento desta tese.

Ao meu "co-orientador", Ricardo da Silva Mendes, por todos os conselhos e recomendações.

À minha família, especialmente, aos meus pais e à minha irmã, pela motivação e acompanhamento ao longo da vida.

A todos os que, de alguma forma, estiveram presentes e contribuíram para completar esta etapa do meu percurso.

Este trabalho é suportado pelos projetos SWING2 (PTDC/EEI-TEL/3684/2014) e Mobiwise (P2020 SAICTPAC/001/2015), financiado pelos Fundos Europeus Estruturais e de Investimento (FEEI) Europeus através do Programa Operacional Competitividade e Internacionalização - COMPETE 2020 e por Fundos Nacionais através da FCT - Fundação para a Ciência e a Tecnologia no âmbito do projeto POCI-01-0145-FEDER-016753, e pelo Fundo Europeu de Desenvolvimento Regional.

This page is intentionally left blank.

Abstract

Location-Based Services are increasingly present in our daily lives. However, regardless of the benefits that these services offer to users, the shared data are not always and only used for the initial purpose. These data can be made public or sold, for example, for commercial purposes. The fact that location data contain information that can reveal the person's identity, routines and habits, raises serious privacy concerns. In order to respond to this problem, there are privacy-preserving mechanisms, namely, for obfuscation and for anonymization of data. However, the correlation between location reports, which can potentially be used by an adversary to estimate the position of the user, has been underlooked in privacy protection. The aim of this thesis is to develop a user-centric Location Privacy-Preserving Mechanism, that is, a mechanism that protects privacy of a user at collection time. In addition, it is intended to protect the users not only against single reports, but also over time, against continuous reports. In this latter scenario, we intent to develop a protection mechanism that is suitable to different frequency of updates and/or to the correlation between reports as to mitigate possible privacy violations that advent from exploring these intrinsic characteristics of location data. Towards this end, we started by evaluating the impact of the frequency of updates on location privacy. For that, we implemented a state-of-the-art tracking attack that allows us to assess the effect of the frequency of updates by estimating the exact user locations. According to the performed analysis, we developed a new mechanism based on geo-indistinguishability that creates obfuscation clusters to aggregate closer locations. This developed mechanism is designated clustering geo-indistinguishability. To evaluate the utility of the mechanism, we resorted to a real use-case based on geofencing. Lastly, the evaluation of the mechanism enables us to conclude that it safeguards the level of privacy and the utility of continuous reports of location data, in a way that it can still be used for the purpose of a service.

Keywords

Location Privacy, Location Privacy-Preserving Mechanisms, Location-Based Services, Geo-Indistinguishability, Clustering

This page is intentionally left blank.

Resumo

Os serviços baseados em localização estão cada vez mais presentes no nosso quotidiano. No entanto, apesar do benefício que estes serviços oferecem aos utilizadores, os dados partilhados nem sempre são usados apenas com o propósito inicial. Estes dados podem ser tornados públicos ou vendidos, por exemplo, para fins comerciais. O facto dos dados de localização conterem informações passíveis de revelar a identidade, as rotinas e os hábitos de uma pessoa, levantam sérias preocupações de privacidade. Para dar resposta a este desiderato, existem mecanismos de preservação de privacidade, nomeadamente, de ofuscação e anonimização dos dados. Contudo, a correlação entre os dados de localização partilhados, que pode ser usada por um adversário para estimar a posição de um utilizador, tem sido negligenciada na proteção da privacidade. O objetivo desta tese é desenvolver um mecanismo de preservação de privacidade de localização centrado no utilizador, isto é, um mecanismo que proteja os utilizadores no momento da partilha de dados. Para além disso, pretende-se proteger o utilizador não só quando este reporta localizações únicas, mas também ao longo do tempo, isto é, quando reporta localizações de modo contínuo. Neste último cenário, pretendemos desenvolver um mecanismo de proteção que seja adequado a diferentes frequências de atualização de localização e/ou à correlação existente entre as localizações partilhadas, de modo a mitigar possíveis violações de privacidade que advenham da exploração destas características intrínsecas dos dados de localização. Neste sentido, começámos por avaliar o impacto da frequência na privacidade de localização. Para tal, implementámos um ataque considerado estado da arte que permite localizar o utilizador ao longo do tempo e do espaço, viabilizando a avaliação do efeito da frequência através da estimação da localização exata do utilizador. De acordo com a análise efetuada, desenvolvemos um mecanismo novo baseado em *geo-indistinguishability* que cria áreas de ofuscação para agregar localizações próximas. O mecanismo desenvolvido é designado *clustering geo-indistinguisahbility*. Para avaliar a utilidade do mecanismo, utilizámos um caso de uso real baseado em *geofencing*. Por fim, a avaliação do mecanismo permitiu-nos concluir que este salvaguarda o nível de privacidade e a utilidade dos dados, de tal modo que continuam a poder ser usados para o propósito do serviço.

Palavras-Chave

Privacidade de Localização, Mecanismos de Preservação de Privacidade de Localização, Serviços Baseados em Localização, *Geo-Indistinguishability*, *Clustering*

This page is intentionally left blank.

Contents

Acronyms

AOI Area of Interest. xv, 16

AOR Area of Retrieval. xv, 16

CR Cloaking Region. 6, 11

DB Database. 14

FN False Negative. 38

FNR False Negative Rate. 40

FP False Positive. 38

FPR False Positive Rate. xvi, 38, 40, 41

GDPR General Data Protection Regulation. 1

GPS Global Positioning System. 5, 23, 25

HMM Hidden Markov Model. 11, 22, 23

LBS Location-Based Service. xv, 2, 5, 6, 9, 11, 12, 14–16, 23, 43, 53

LPPM Location Privacy-Preserving Mechanism. 2, 3, 5, 6, 8–10, 13, 15, 17, 19, 20, 23, 27, 29, 31–33, 40, 43, 44

MAD Median Absolute Deviation. 27

MLE Maximum Likelihood Estimator. 10

MM Map-Matching. 9–11, 19, 21–25, 27–29, 34, 44, 55

PEBA Profile Estimation Based Attack. 10

PL Planar Laplace. xvi, 6, 7, 19–21, 28, 31, 32, 34–38, 40–43

PoI Point of Interest. xvi, 2, 16, 38–41

TN True Negative. 38

TNR True Negative Rate. 40

TP True Positive. 38

TPR True Positive Rate. xvi, 38, 40–42

This page is intentionally left blank.

List of Figures

List of Tables

This page is intentionally left blank.

Nomenclature

x_i	Exact user location at timestamp i
z_i	Obfuscated location at timestamp i
$\hat{x}_i$	Adversary's estimated location at timestamp i
t_i	Time at timestamp i
$\mathbf{x}$	Vector of all real locations
$\mathbf{z}$	Vector of all obfuscated locations
$\hat{\mathbf{x}}$	Vector of all estimated locations
$\mathbf{x}_i$	Vector of real locations up to timestamp i
$\mathbf{z}_i$	Vector of obfuscated locations up to timestamp i
$\hat{\mathbf{x}}_i$	Vector of estimated locations up to timestamp i
$\mathcal{X}$	Set of all possible real locations
$\mathcal{Z}$	Set of all possible obfuscated locations
$\hat{\mathcal{X}}$	Set of all possible estimated locations
Δ_t	Minimum interval between consecutive reports
$f(\cdot)$,$p(z_i\|x_i)$	General Location Privacy-Preserving Mechanism (LPPM)
ϵ	Geo-indistinguishability privacy parameter
$h(\cdot)$, $p(\hat{x}_i\|o_i)$	General adversary's attack
$P_{AE}(h, \mathbf{x}, \mathbf{z})$	Average adversary error of $\hat{\mathbf{x}}$ given $\mathbf{z}$ and h
$Q(f, \mathbf{x}, \mathbf{z})$	Quality loss given the LPPM f and locations $\mathbf{x}$
$d(\cdot)$	Euclidean distance metric
$g(\cdot)$	Great-circle distance
o_i	Location observation (noisy GPS reading) at timestamp i
$\mathbf{o}$	Vector of all location observations (noisy GPS readings)
$s_{i,k}$	k^{th} candidate location for o_i at timestamp i
$p(o_i\|s_{i,k})$	Map-matching emission probability
$p(s_{i,k}\|s_{i-1,j})$	Map-matching transition probability

σ	Standard deviation of the measurement error
λ_y	Parameter for the exponential of the measure of circuitousness
λ_z	Parameter for the exponential of the measure of temporal implausibility

Chapter 1

Introduction

1.1 Motivation

Nowadays, our personal information is exposed to possibly untrustworthy entities which have the capacity to share the data collected with third parties. Although the analysis of this data may be beneficial to several services and, hence, to consumers, much of the collected data contains sensitive and private information, which raises privacy concerns.

Recently, the newspaper *The New York Times* published an article entitled "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret" [1] mentioning that "Every moment of every day, mobile phone apps collect detailed location data". This interesting article exemplifies exactly one of the motivations of this thesis. It shows how the data collected by the applications become public and it describes some cases that prove the possibility of identifying a person by accessing those public data. For example, Lisa Magrin is a math teacher, whose location information was gathered by a mobile app which sold those data without her knowledge. The New York Times disclosed Ms. Magrin's identity by accessing the database. The app tracked every place she had been. Through her location information was possible to reveal the path from home to work and the visit to a doctor's office and, specifically, the time spent there. The article also tackles the lack of information on data collection given by apps to users and, the most worrisome, the lack of people awareness in the context of privacy.

In another privacy-breach example, Vines *et al.* showed how online advertisement can be used to track the users' location and to have information about the installed applications [2]. The author showed that it is possible to create targeted advertising that allows to perform privacy attacks for as little as 1000 USD. From the collected information, it is possible to know as the users move from home to work and to other privacy sensitive locations (e.g. hospitals or treatment/abortion centres). Moreover, it is possible to infer about the interests of the users based on the installed applications and, therefore, acquire personal information without user consent.

Privacy has been recognised as a people's right and is enshrined in the Universal Declaration of Human Rights [3] (Article 12), the European Convention on Human Rights [4] (Article 8) and the European Charter of Fundamental Rights [5] (Article 7). However, the right is defined in a restrict scope. According to Article 12, it only mentions that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence". Furthermore, the European Union General Data Protection Regulation (GDPR) [6] was reshaped and since May 2018 it has been applied to all members of the European Union. Personal information, according to GDPR, is "any information relating to an [...] identifiable natural person". Nevertheless, considering that location data as personal information depends on the context, the GDPR is not clear on the definition of location data privacy.

Despite the aforementioned, there is not a standardised and universal definition of privacy. Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" and as "the ability of an individual to control the terms under which personal information is acquired and used" [7]. Considering these definitions, the notion of information's privacy consists in having control of the personal data collected and handled by others entities.

This thesis will focus on the privacy of the users' location, which is part of the personal information that can be collected by services. According to Blumberg and Eckersley, location privacy "is the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use" [8]. In this sense and due to the attractiveness of Location-Based Services (LBSs), which have proliferated as a result of the ubiquitousness of mobile devices, the preservation of privacy of location data is becoming an emerging topic. LBSs consist in services in where users share their location over time in exchange for geographically and/or temporally related information, such as, finding nearby Points of Interest (PoIs). However, regardless of the benefits for the user, this flow of information poses a threat to their privacy. The providers of the services and the entities with whom they share data have the opportunity to track the users' location and use it maliciously [9].

The collection of users' locations grants to service providers the constitution of datasets that can become public or shared with third-parties for financial or research purposes. Furthermore, dataset leakage is always a possibility. To prevent unwanted disclosure and, hence, to protect/anonymize users' location, a Location Privacy-Preserving Mechanism (LPPM) is required. Nevertheless, considering informed adversaries can perform data deanonymization, the datasets can often be leveraged, even if the datasets are fully anonymized [10]. This is specially critical for location data because human mobility traces are highly unique and extremely predictable given that visited locations possibly reveal the user's identity, habits, addictions or even health conditions [11, 12, 13].

The considerations mentioned above constitute the main challenge motivating this work. The objective of an LPPM is to preserve a certain level of privacy which can come at the expenses of a degraded quality of service. LPPMs can be applied in different phases of the data lifecycle, namely: data collection, data publishing, data distribution and at the output of the data mining [14]. In this research, the focus will be the phase of data collection, where the protection mechanisms can be categorised as anonymization, obfuscation and cryptographic techniques [11, 15]. Mechanisms that run at collection time, meaning, run in-device before sharing data with providers, empower the users to have control over data instead relying on possibly untrustworthy providers. In addition, the users are able to choose the characteristics of the protection mechanism according to their privacy preferences. Therefore, and since the privacy mechanism protects each user independently, these mechanisms are referred to as user-centric LPPMs [16].

Depending on the LBS, location data can be reported either continuously or rather sporadically [17, 18]. The frequency of reports impacts directly the temporal correlation between subsequent reports, which in turn can be used by an adversary to track users over time and even predict future locations [11, 15, 19]. While some recent research has started considering temporal and spatial correlations [19, 20], this topic is far from being mature and is still considered an open issue [15]. In fact, in the context of sporadic release of data, LPPMs typically consider reports to be independent between each other [17]. Therefore, we will explore this intrinsic characteristic of location data from the perspective of privacy protection by proposing a user-centric LPPM that acts at collection time and that is suitable for continuous reports of location data.

1.2 Objectives

The main goal of this thesis is to develop a user-centric LPPM in order to protect users at collection time. This goal is divided into the research objectives explained below.

The first research objective is to improve understanding of the existing LPPMs, attacks and metrics of privacy and utility. This allows us to obtain insights about the focus of previous works, the aspects that an LPPM or an attack should take into account, as well as the analysis performed by them. Currently, the research community is beginning to consider the temporal and spatial correlations in location data [15], which leads us to the second objective.

The second research objective is to evaluate the impact of the frequency of updates in the privacy and utility of protection mechanisms and attacks. Commonly, the geo-temporal correlation between reported locations is used as an attack against location privacy. Our intention is to understand how temporal correlation influences the mechanisms' performance and, more specifically, the privacy of users under attack.

Hereupon, the third research objective is the development of a privacy-enhancing mechanism that is suitable to different frequency of updates and/or to the correlation between points. This objective focuses on tackling the impact that the frequency of updates can have on privacy, as mentioned previously.

Lastly, the fourth research objective is the implementation and evaluation of the mechanism taking into account the privacy level and the utility metrics. Our focus is the development of an LPPM that safeguards the level of privacy and the utility of data, in a way that can still be used for the purpose of the service.

1.3 Contributions

From the developed work on this thesis, we submitted the following scientific article to the conference *MobiQuitous 2019*:

- Ricardo Mendes, Mariana Cunha and João P. Vilela. Impact of Frequency of Location Reports on the Privacy Level of Geo-indistinguishability. In *16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. 2019.

This article reports the evaluation of the impact on the privacy level of geo-indistinguishability under different frequencies of report. To do so, the privacy level of a geo-indistinguishable LPPM was measured against state-of-the-art localisation attacks and a tracking attack for different frequencies of updates, using two real mobility datasets. Part of the work performed in this thesis went into this article, in particular the selection and the pre-processing of one of the mobility datasets, the implementation of the tracking attack, and the results and respective analysis of the effect of the frequency of reports on this attack.

1.4 Thesis Structure

This thesis is structured in 5 chapters, whose contribution is summarised in this section. The current chapter provides an overview of the thesis, specifying the motivations, the objectives, the research contributions and the structure of the document. Chapter 2 describes the state of the art by explaining the privacy protection mechanisms, the mechanisms to compromise location privacy and the metrics of privacy and utility. Following, in Chapter 3 is presented the work developed during the first semester, such as the implementation of the LPPMs and the attacks, and the evaluation of the impact of frequency of reports on them. Chapter 4 describes the proposed mechanism, the performed analysis and the

obtained results. Finally, Chapter 5 draws the final conclusions and presents some ideas for future work.

The work plan of the thesis is presented in Appendix A. In this appendix, we describe the work plan for the first semester and for the second semester, including the scheduled tasks and the Gantt charts for each semester.

Chapter 2

State of the Art

Location privacy, Location-Based Services (LBSs), and location information are concepts briefly presented in this chapter as background knowledge. Then we will discuss the state of the art of the following topics: privacy protection mechanisms for location data (see Section 2.1), mechanisms to compromise location privacy (see Section 2.2), and metrics of privacy and utility (see Section 2.3).

Location privacy is an emerging topic of research [11, 15, 21] due to the pervasiveness of LBSs and always connected mobile devices. Figure 2.1 presents a system model of an LBS, with its main components. In these systems, users obtain their location through a positioning system, such as a Global Positioning System (GPS), using their devices (e.g. smartphones). The location is then sent through a network to either a location privacy server, where an Location Privacy-Preserving Mechanism (LPPM) is applied to the data, or directly to an LBS server. After being applied an LPPM, the privacy server also passes the data to the LBS server. The LBS then uses a content/data provider to retrieve information related with the location of the user which is then sent back through the network to either the user or to the privacy server, which then redirects it to the former. It should be mentioned that a privacy server is optional, and in fact, depends on the LPPM used by the user. User-centric LPPM typically run in-device. Furthermore, both the content/data provider and the location privacy server can be owned by the service providers or by third parties.

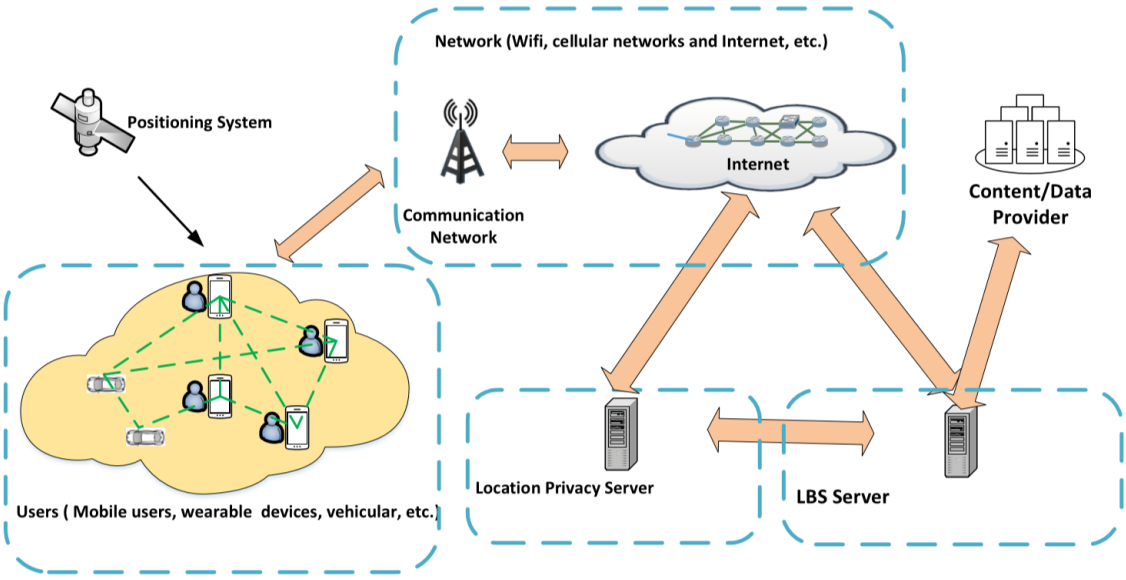


Figure 2.1: System model of an LBS (adapted from [15]).

Wernke *et al.* defined location information as a tuple ⟨*identity, position, time*⟩ [21], where identity is a property or a set of properties identifying the user, position is the exact location of a user, and time is the point in time when the information was reported. Considering these attributes, the user may choose which of them must be protected or revealed. Their work discusses different approaches based on the protection goal chosen by the user. The focus of this thesis will be the protection of the user's position, taking into account the time between the reports, in other words, the frequency of updates. Commonly, the approach to protect the user's location is the use of obfuscation mechanisms [15, 21], whose state of the art will be presented in Section 2.1.

Shokri *et al.* classified LBSs as continuous or sporadic depending on the frequency of location reports [17]. An LBS is considered continuous when the user's location is reported periodically, and it is considered sporadic when the user requests a single location query, receives the result from the service and then terminates the query. Therefore, the study of the state of the art of the mechanisms presented in Sections 2.1 and 2.2 will be based on this classification.

2.1 Privacy Protection Mechanisms for Location Data

Considering the focus of this thesis, this section provides a study of the state of the art of privacy protection mechanisms for obfuscation of location data at collection time. The existing LPPMs have been developed for both continuous [16, 19] and sporadic scenarios [22, 23, 24], depending on whether they consider the dependence or independence of the temporal correlation between subsequent reports, respectively. Earlier research focused on the sporadic scenario, whereas recently, studies on continuous reports have been emerging. Thus, the discussion in this section will address these mechanisms chronologically.

Kido *et al.* proposed the first method of dummy-based privacy protection [25, 26], for sporadic scenarios. In this method, the users generate a set of false positions, also known as "dummies", for their real position. Both the generated dummies and the users' real location are sent to the LBS provider, which cannot distinguish or identify the user's real position. In these works, the authors performed a comparison among the number of dummies, the size of the region where the dummies are generated, and the obtained location anonymity. They concluded that their proposed method protects the location of the users and that a higher number of dummies corresponds to higher protection of the user's location. However, the generation of the dummies can be hard, since they should be realistic enough through space and time, or otherwise, the dummies could be easily identified [20].

Location cloaking is an approach that protects the users' location when they access LBSs [27, 28]. This approach consists in replacing the users' real location with a Cloaking Region (CR) that encloses their real position. Ghinita *et al.* proposed a technique, based on CRs, that protects the users against adversaries that use prior knowledge about the maximum user velocity to perform linkage attacks [29], that is, attacks in where additional information is used to better locate/identify the user. The results obtained by the authors showed that the proposed mechanism achieves privacy without a significant quality of service degradation.

Geo-indistinguishability is a proposed LPPM for sporadic scenarios, based on the classic notion of differential privacy [22]. As shown in Figure 2.2, this LPPM guarantees the users' privacy within a radius r, making any disclosed location indistinguishable from any other point within that radius. The privacy level achieved depends on the r and to be achieved, the mechanism adds controlled random noise to the user's position. The Planar Laplace (PL) mechanism was the first geo-indistinguishable LPPM proposed. The PL mechanism adds 2-dimensional Laplacian noise centred at the exact user's location x

following a Laplacian distribution. Figure 2.3 shows the probability density function (pdf) of two PL functions, that is, the probability of generating a point z around the exact user location x. For two users' locations x, x', the PL mechanism forces the corresponding distributions to be at most $\epsilon d(x, x')$ distant [30]. The $d(\cdot)$ is naturally used as Euclidean metric for location privacy, since we would like two points to be more distinguishable when they are geographically closer [30]. Regardless of the efficiently draw of the noise by the PL mechanism, in order to increase the utility of the data without decreasing the level of privacy, remapping techniques have been proposed [23]. Currently, the PL mechanism with optimal remapping is considered the state of the art of geo-indistinguishability in sporadic location privacy [24].

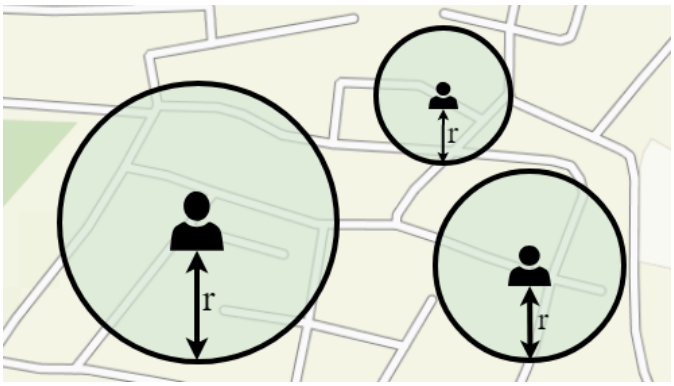


Figure 2.2: Example of geo-indistinguishability.

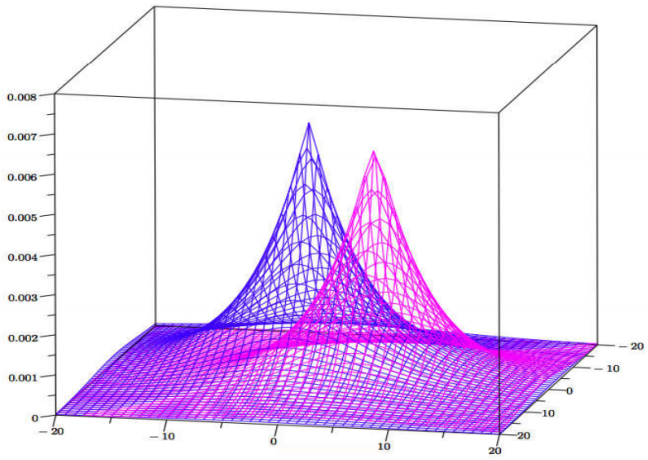
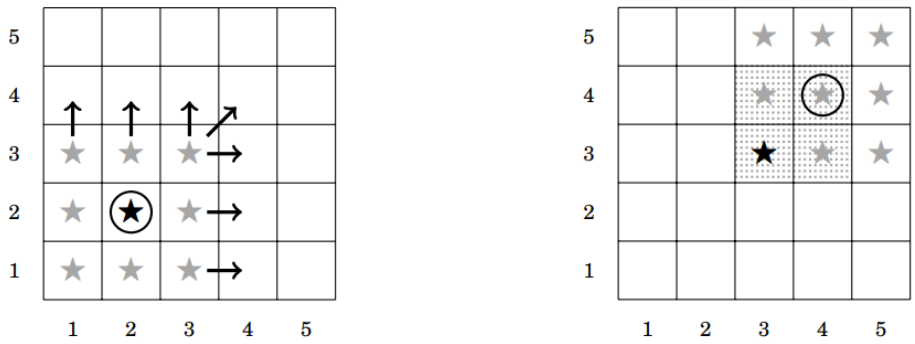


Figure 2.3: Example of the probability density function of two planar Laplacian functions, centred at (-2,-4) and at $(5, 3)$ respectively, with $\epsilon = 1/5$ (from [22]).

Chatzikokolakis *et al.* proposed a mechanism also based on differential privacy - a predictive mechanism [31]. This work showed how correlations in traces can be used to predict the next user's location based on previous reports. To predict the user's location, the mechanism uses a private test which evaluates the quality of the predicted location. If the test is successful the predicted location is reported, otherwise, a new predicted location is generated with new noise. Regardless of the benefit of this mechanism and its efficient way of drawing noise, if there is not a considerable correlation in the trace, the private test can be considered an extra cost to the mechanism and can degrade its efficiency. Moreover, this work suggests as future research determining the necessary time to break the correlation in traces.

Also based on differential privacy, Xiao and Xiong proposed a solution to preserve location privacy in continuous scenarios, under temporal correlations, and with strong privacy guarantees [19]. This work provided a new definition of "δ-location set" to consider temporal correlations in location data. They defined δ-location set as a set of probable locations where the user might be at each timestamp, disregarding locations with small probabilities. The authors of [19] defined this probability as the prior probability of a user's location at each timestamp t and, hence, a δ-location set contains the minimum number of locations with prior probability sum no less than $1 - \delta$.

Shokri *et al.* proposed "a methodology that enables the design of *optimal* user-centric location obfuscation mechanisms respecting each individual user's service quality requirements" [16]. This methodology considers both the user's objective, maximising location privacy, and the adversary's objective, minimising localisation error, which makes the solution optimal. Based on this, the authors of [16] developed two linear programs to optimise both objectives, maximise the user's objective and minimise the adversary's objective. Moreover, the LPPM developed by them deals with the correlation between past, current and future user's location. The aim of their LPPM is to protect the current location without compromising the privacy of past locations, while maintaining the current obfuscation compatible with potential future locations, that is, from the current location it is still possible to reach a future location. As shown in Figure 2.4, attacker's uncertainty can be reduced when temporal correlation is disregarded.



(a) Time $t-1$: real location (2,2) (★); exposed obfuscated location (2,2) (◯). As (2,2) was exposed, the user can only be in the bottom left 3x3 square (★). Since the user moves only to adjacent locations, at time t she will be in the bottom left 4x4 square.

(b) Time t: real location (3,3) (★); exposed obfuscated location (4,4) (◯). As (4,4) was exposed, the user can only be in the top right 3x3 square (★). However, the correlation with the previous disclosure implies that the user can only be in the dotted 2x2 square.

Figure 2.4: Example of how the correlation of user's locations between times $t-1$ and t reduces attacker's uncertainty about the user's current location (time t) (from [16]).

Liu *et al.* provided a filter of dummies to be applied to existing dummy-based methods [20]. Recall that these methods append fake locations, also known as "dummies", to the exact user locations. The provided filter considers the spatiotemporal correlation from the three following aspects: time reachability, direction similarity and in-degree/out-degree. Time reachability consists on checking if the location C_i is reachable from location C_{i-1} in the time interval between these locations. Direction similarity is used to compare the similarity of the angle between the reachable fake path and real path in movement direction. Finally, in-degree/out-degree consists in the binomial in-degree and out-degree, where in-degree corresponds to the number of movement paths which end at the location C_i and the out-degree corresponds to the number of the movement paths which start from the location C_{i-1}. The dummies generated will be reported if and only if they are feasible from the

previous location. Moreover, the results given by the authors showed that the proposal is effective and efficient. Figure 2.5 presents an example of spatiotemporal correlation, where it is possible to perform the following analysis: (a) the LBS provider infers that C_i is a dummy because, as there is a lake, the user cannot move from $A_{i-1}, B_{i-1}, C_{i-1}$ or D_{i-1} to C_i; (b) the LBS provider identifies A'_{i-1} as a dummy because it is in the opposite direction of the other reported locations, and, additionally, as there are three movement paths from the set Loc'_{i-1} to C'_i the LBS provider can assume with a high level of confidence that C'_i is the user's real location.

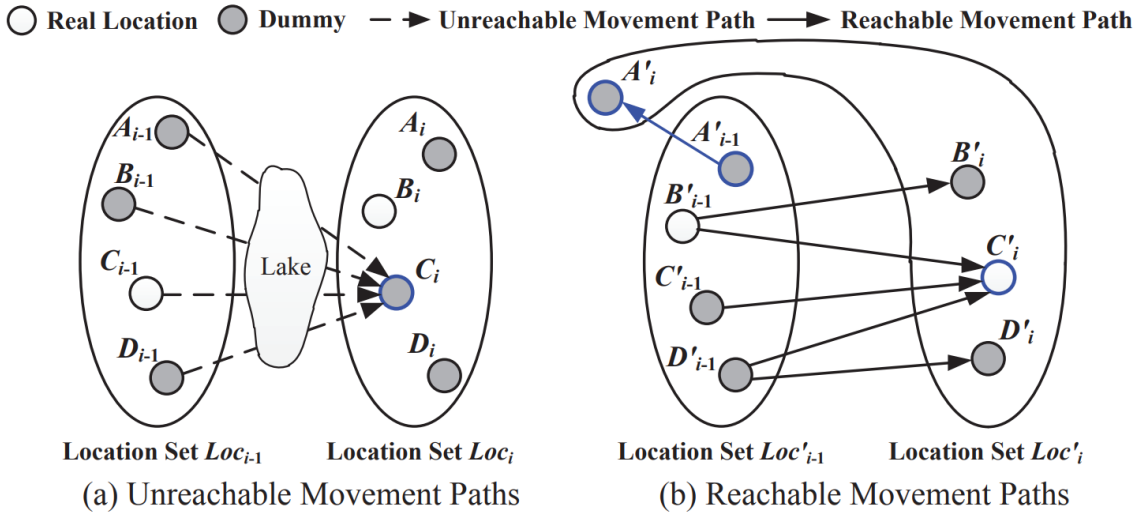


Figure 2.5: Example of spatiotemporal correlation (from [20]).

Recently, an adaptive geo-indistinguishability mechanism was proposed for continuous scenarios [32]. This work explores the effect of the correlation among the user's obfuscated locations on a certain privacy level and proposes an adaptive LPPM. This mechanism considers the correlation level of the previous obfuscated locations $\mathbf{z}$ to adjust the amount of noise required to obfuscate the exact user location x. The noise will be added if the privacy level increases and, otherwise, the noise will be reduced to improve the utility level. The results obtained by the authors showed that the adaptive mechanism achieves better performance by adjusting the noise added according to the correlation of previous obfuscated locations.

2.2 Mechanisms to Compromise Location Privacy

This section provides the state of the art of mechanisms to compromise location privacy, in other words, location privacy attacks. The existing attacks can be classified depending on the adversary knowledge [21]. Specifically, the authors of [21] divided the attacker knowledge into temporal information, if the attacker accesses a single user's position or to the information history (e.g. a set of collected positions during a trajectory), and context information, when the attacker has context knowledge beyond the spatiotemporal information (e.g. a map or a phone book).

Based on the attacker knowledge, the authors of [21] provided a classification of attacks of location data and of all the other attributes of location information. Considering the focus of this thesis, the classified attacks that can be applied to location data are the following: *probability distribution attacks* [18], where the attacker infers a probability of the user's position over the obfuscation area, based on additional context information (e.g. traffic statistics); *Map-Matching (MM)* [33], whereby the attacker restricts the obfuscation area

by removing areas where the user cannot be located; *region intersection attacks* [34], when the user takes advantage of imprecise reported position updates or queries from a user to calculate their intersection; and *maximum movement boundary attacks* [29], where the attacker calculates the maximum movement boundary area to infer where the user could have moved between two subsequent reports.

Notwithstanding, to choose an attack the adversary should define its target first. According to [15], *sensitive place attacks* (position attack) are chosen when the attacker wants to disclosure important user's locations, *presence and absence disclosure attack* (position and discrete time attack) when the attacker wants to determine if a user is localised or not at a place at a certain time, and *tracking attack* (position and continuous time attack) when the attacker follows a user over time and space. *Sensitive place attacks* are also known as inference attacks [33] and *presence and absence disclosure attack* are also known as localisation attacks [17]. The localisation and tracking techniques are the most generic type of attacks in the context of user-centric location privacy [17]. Similarly to the LPPMs, these two types of attacks consider continuous and sporadic scenarios, respectively.

Considering the focus of this thesis, the relevant mechanisms to take into account should attack the position and the time attributes. Based on this, we now discuss the state of the art of localisation attacks and tracking attacks.

2.2.1 Localisation Attacks

Localisation attacks are more suited for sporadic data, since they consist in localising a user at a certain place and at a certain period in time. Shokri *et al.* developed an optimal attack for an attacker that has prior knowledge in the form of a mobility model [35]. This attack considers the optimisation of the adversary's objective, which is the correctness of the resulting location, by minimising the average estimation error. The results obtained by the authors showed that the optimal localisation attack proposed outperforms a Bayesian inference attack. This latter attack was also proposed by Shokri *et al.* and consists in a localisation attack using Bayesian inference for Hidden Markov Processes [17].

Recently, Oya *et al.* proposed an optimal attack, Profile Estimation Based Attack (PEBA), that learns the user mobility profile as the user reports locations [24]. The PEBA is based on a blank-slate model, which starts as a *tabula rasa*, only with probabilistic information about the mobility profile π, computed from the training set. To acquire additional information about this mobility profile π, the attacker uses both the user's real locations $\mathbf{x}$ and user's obfuscated locations $\mathbf{z}$ observed. Considering this mobility model, the attacker's knowledge of π will be adapted after each query, which will be used to design and to perform the attack. The PEBA attack was designed by decomposing the estimation problem of user's location x given the obfuscated locations $\mathbf{z}^r$ into two steps. First, they use the Maximum Likelihood Estimator (MLE) to estimate the mobility profile of the user, knowing the user's obfuscated locations $\mathbf{z}^r$. Second, given the obfuscated locations $\mathbf{z}^r$, they estimate the user's real location x assuming it follows the distribution given by $\hat{\pi}^r_{ML}$, which is the MLE of the mobility profile π in the *r-th* query. Furthermore, the authors of [24] showed that PEBA outperforms optimal attacks developed for hardwired models of user mobility, when evaluated on data not used for training [23, 36].

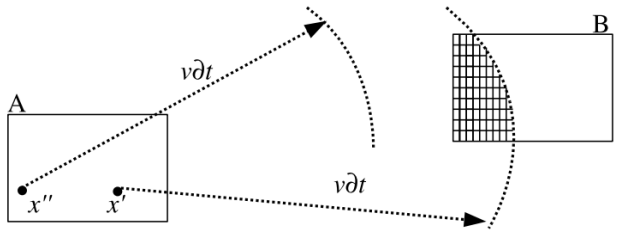
2.2.2 Tracking Attacks

Tracking attacks are better suited for continuous data, since they consist in following a user over time and space. MM is a technique used to localise a vehicle continuously on a road network given noisy readings. Currently, there are three major surveys on MM [37, 38, 39]. The most recent survey [39] provides a selection and classification of existing MM applications. Moreover, the authors performed an analysis of the trade-offs to consider

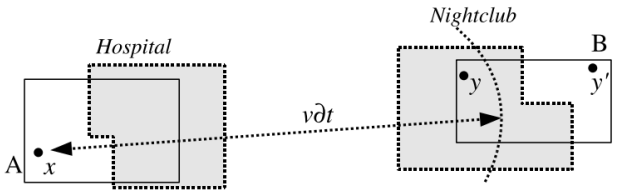
when choosing a MM method and selected guidelines to help this choice. Generally, the MM approaches are classified as low-sampling and high-sampling, depending on the frequency of updates. In the context of MM, it is typically considered high frequency of updates when reports are made up to every 1 minutes or least and low frequency techniques are evaluated up to a maximum of 5-6 minutes [38]. However, in the context of LBSs there is no formal nor quantitative boundary for the frequency of updates that defines what intervals belong to the low-sampling or high-sampling scenarios.

Newson and Krumm provided a MM algorithm that uses a Hidden Markov Model (HMM) to find the route represented by a sequence of points [40]. Moreover, their solution considers noisy readings and sparse location data. The results obtained by the authors showed how the accuracy of their method degrades when the frequency of updates decreases and when the level of noise increases. This work is mentioned in [39] as a popular method and considered by [41] as the state of the art. However, recently, Jagadeesh and Srikanthan developed a MM solution for noisy and sparse location data to be applied in an online way [41]. Their method is based on a HMM and on a route choice model, which considers real driving data. The results obtained by the authors showed that their solution achieves a higher accuracy when compared with the state-of-the-art algorithms [40], even at high levels of noise.

Ghinita *et al.* tackled an attack for continuous scenarios that considers an adversary with prior knowledge about the maximum user velocity [29]. In their work, they considered two attackers showed in Figure 2.6. In (a), the attacker does not have access to information about the sensitive locations on the map, and wants to ensure that the user can reach some point in Cloaking Region (CR) B from any point in CR A. In (b), the attacker has information about sensitive locations, and wants to ensure that the user can reach any point in CR B from any point in CR A. Based on these attackers, the authors proposed a mechanism that protects the users against them.



(a) Adversary without background knowledge



(b) Adversary with background knowledge

Figure 2.6: Attack model (from [29]).

2.3 Metrics of Privacy and Utility

This section gives an overview on privacy metrics (see Section 2.3.1), utility metrics (see Section 2.3.2) and, lastly, a brief discussion on the trade-off between privacy and utility (see Section 2.3.3).

2.3.1 Privacy Metrics

In order to quantify the level of privacy, several metrics have been proposed. However, finding a standard for evaluating privacy remains a challenge, because there are multiple definitions of privacy. In this section, relevant works in this context will be presented.

The systematic survey of Wagner and Eckhoff provides an elaborated summary of privacy metrics, not only in the scope of location privacy but in the general domain of privacy [42]. This work covers more than eighty privacy metrics and introduces categorisations based on the following: the aspect of privacy to measure, the required inputs, and the type of data to protect. The defined categories group the metrics by the outputs they measure as follows: uncertainty, data similarity, time, error, information gain/loss, indistinguishability, adversary's success probability, and accuracy/precision. Each of the categories has associated some privacy metrics, however, most of them are not considered in location privacy domain.

Wagner and Eckhoff further present a set of nine questions that helps in the choice of the right privacy metrics for a specific case. In the survey, the selection of questions is followed by an explanation about the aspects considered and these questions are also followed by information to take into account in the answer. Next, the questions from [42] will be transcribed:

- ***Suitable Output Measures?*** *Which aspects of privacy do we want to quantify? Do we want to give privacy guarantees, or is some loss of privacy acceptable?*
- ***Adversary Models?*** *What are the characteristics of the adversary we consider? How do we incorporate the adversary's goals and their knowledge?*
- ***Data Source?*** *Which data sources do we aim to protect?*
- ***Availability of Input Data?*** *Which types of input data do we want to consider, and which are available in our scenario?*
- ***Target Audience?*** *What is the intended audience for our study? What are their expectations regarding the presentation of results, and do they understand the interpretations of our metrics?*
- ***Related Work?*** *Which metrics are used by work that is related to ours, and would those metrics be suitable in our work as well? Which mathematical concepts or formalisms are used by others in our field? Which of these are already available in the tools we use?*
- ***Quality of Metrics?*** *Do any of the candidate metrics have known flaws? Is it feasible to conduct a study that verifies that candidate metrics indeed behave as we intend?*
- ***Metrics Implementations?*** *Are there implementations of the candidate metrics that we can use, or compare our implementation with?*
- ***Metrics Parameters?*** *How should we choose the parameter values for the candidate metrics?*

Although the survey gives a summary of privacy in general, they mention the possibility to use metrics from other domains or to combine different metrics. In the domain of LBSs, they refer the work of Shokri *et al.* [18]. This work considers that location privacy, as shown in Figure 2.7, should take into account the following three aspects: accuracy, certainty and correctness. These aspects correspond to how accurate, how certain and how correct the adversary's estimations are.

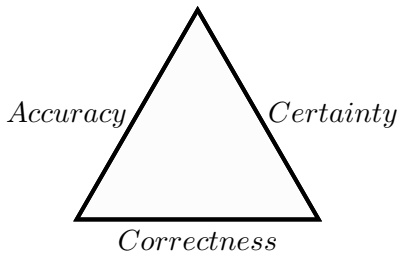


Figure 2.7: Triangle for metrics of Privacy (adapted from [18]).

To quantify location privacy, the authors developed a framework that allows the analysis of LPPMs. They also proposed and justified the right metric to determine users' privacy and explained some other metrics used in the context of location privacy, namely: k-anonymity and entropy.

In summary, the analysis performed by Shokri *et al.* showed that correctness is the right metric to measure users' privacy. Considering that certainty measures the success of an attack and that maximum accuracy of adversary's estimations can be achieved under resource constraints, neither of them allows the evaluation of an LPPM. To evaluate an LPPM, it must be considered the exact location x and the adversary's estimation $\hat{x}$, in order to measure the adversary's correctness, which determines the privacy of users.

Conversely to the work of Shokri *et al.* [18], Oya *et al.* [36] have recently justified the use of other metrics, such as conditional entropy, as auxiliaries to the design of LPPM. In fact, they show that these complementary criteria are essential as no mechanism fares efficiently in all privacy domains.

Liu *et al.* performed a recent systematic study on *Location Privacy and Its Applications* [15], where the works described above [18, 42] are also referred, and classified location privacy metrics into five categories, as explained below. Although Shokri *et al.* mention accuracy as a metric, Liu *et al.* dismiss it, since it is not commonly used.

Certainty

Certainty or uncertainty metrics evaluate the ambiguity of adversary's estimations to quantify the success of an attack. A high privacy level is related to a low certainty. Liu *et al.* divided certainty in numerical metrics and entropy-based metrics [15].

The first one concerns to metrics that measure the level of privacy considering the number of points sent by a user with a single location-based query. The privacy level increases with the increasing number of points reported, which means more ambiguity. There are LPPMs that use this type of metrics to evaluate the privacy level achieved. For example, in k-anonymity, k is used to represent the level of privacy [43, 44], as well as p-sensitivity uses p [45] and l-diversity uses l [46]. Briefly, k-anonymity consists in a set of k individuals, where the identity of each person cannot be disclosed from at least k-1 individuals in the same set. The p-sensitive mechanism satisfies the k-anonymity property and guarantees that within a set of k individuals, for each group of confidential key attributes, the number of distinct values is at least p for each confidential attribute within the same group. In the latter example, l-diversity guarantees that the user's position is different from a set of k individuals and the individuals are located distant enough from each other.

The entropy-based metrics evaluate how well an attack can disclose a user's position and an adversary can identify the user. Considering the observations $\mathbf{o}$ and the adversary's

estimations $\hat{\mathbf{x}}$, the entropy is defined by the following equation:

$$\sum_{\hat{x_i} \in \hat{\mathcal{X}}} p(\hat{x}_i|o_i) \log \frac{1}{p(\hat{x}_i|o_i)} \tag{2.1}$$

where $p(\hat{x}_i|o_i)$ is the probability of the adversary's estimation $\hat{x}_i$ to occur given the observation o_i, thus modeling the attack from an adversary. This equation measures how well an adversary can identify a certain user.

Correctness

Liu *et al.* divided correctness in adversarial success rates and distance-based metrics [15]. The adversarial success measures the probability of success of an adversary or, when there is more than one attempt, the percentage of success. The evaluation through this metric depends on the context and, hence, the definition of success also depends on it.

The distance-based metrics are measured by the expected estimation error and quantified using the distance between the exact locations $\mathbf{x}$ and the adversary's estimations $\hat{\mathbf{x}}$. Considering observations $\mathbf{o}$, adversary's estimations $\hat{\mathbf{x}}$, and a distance metric $d(\cdot)$, typically the Euclidean distance [35], the expected estimation error is defined by the following equation:

$$\sum_{\hat{x_i} \in \hat{\mathcal{X}}} p(\hat{x}_i|o_i) d(x_i, \hat{x}_i) \tag{2.2}$$

Information Gain or Loss

These metrics quantify the amount of information gained by an adversary, which corresponds to the amount of privacy lost by users. The increase of user's privacy depends on the least information an adversary can gain. In this context, Liu *et al.* defined a new privacy metric, privacy degree, as the percentage of queries responded by the onboard unit (i.e. the communication device mounted on vehicles) [47]. In fact, an onboard unit works as a cached content in the local memory, which is more secure than using an LBS server. According to [47], privacy degree corresponds to the percentage of queries made by the users and responded by the cached content instead of the service provider.

Geo-Indistinguishability

Indistinguishability is recognised as a classic notion in the security domain. Based on this notion, some metrics were introduced to measure if a pair of outcomes of a privacy mechanism is indistinguishable to an adversary. In this case, a high level of privacy means that an adversary cannot distinguish two outcomes within a given set of outcomes.

In the domain of statistical Databases (DBs), differential privacy was introduced, which guarantees that any disclosure does not consider the presence or absence of an item in a DB [48]. Briefly, differential privacy aims to minimise the risk of an individual or a record entering in a DB, thereby encouraging the participation in data sharing. In particular, the objective of differential privacy is that a DB reveals low information about a certain individual/record, even if all the information about the others is known. That is, the response to a query to the DB must be indistinguishable, whether the individual/record is in the DB or not, which makes the individuals sure about the share of their data. The most common mechanism of protection consists in add noise to the data, in order to provide formal guarantees of privacy. In the domain of location privacy, geo-indistinguishability was proposed based on differential privacy, to guarantee that any disclosed location is

indistinguishable from any other point within a variable radius, which means that the user takes ϵ-geo-indistinguishability [22]. An LPPM f ensures this definition if and only if:

$$d_{\mathcal{P}}\left(f(x), f(x')\right) \leq \epsilon d_{\mathrm{x}}(x, x') \quad \forall x, x' \in \mathcal{X} \tag{2.3}$$

where $d_{\mathrm{x}}(\cdot)$ is a distance function and $d_{\mathcal{P}}(\cdot)$ is the multiplicative distance between two distributions, σ_1 and σ_2, on the same set S, defined as:

$$d_{\mathcal{P}}(\sigma_1, \sigma_2) = \sup_{S \in \mathcal{S}} \left| \log \frac{\sigma_1(S)}{\sigma_2(S)} \right| \tag{2.4}$$

From equation (2.3), for all locations x' within a radius r from the true location x, the probability of generating the obfuscated location z is bounded by the distance of r, which depends on the parameter ϵ. This parameter represents the level of geo-indistinguishability.

Commonly [22, 23], ϵ is set to $\epsilon = l/r$, where r and l are a user specified radius and privacy level, such that for any x, x':

$$\begin{aligned} &d_{\mathrm{x}}(x, x') \leq r \\ &d_{\mathcal{P}}\left(f(x), f(x')\right) \leq l \end{aligned} \tag{2.5}$$

Based on this, for closer x, x' locations the probability functions are forced to be similar, while for distant locations the similarity of probability functions is lower, which allows the service provider to distinguish points far away from each other.

Time

Time-based metrics can be used in two different ways. On one hand, these metrics are used to measure the time until the adversary's success, assuming that the adversary will succeed. In this case, a high level of privacy is related to a long time until the adversary's success [49]. On the other hand, these metrics are used to measure the time until the adversary becomes confused, assuming that the privacy mechanisms will confuse the adversary [28]. In this case, a high level of privacy is related to a short time until the adversary is confused. According to [28], "the time to confusion is the tracking time between two points where the adversary reached confusion (i.e., could not determine the next sample with sufficient certainty)".

2.3.2 Utility Metrics

Despite the importance of the privacy level of an LPPM, the utility of the outcome of a protection mechanism should also be considered. Generally, utility is related to service-quality and can be measured through data quality metrics. In previous works as [23, 35, 50], some metrics have been proposed to measure utility and they will be presented below.

Shokri *et al.* mention that an effective LPPM, beyond the privacy requirements of the users and the adversary's model, should consider the maximum tolerated service quality degradation [35]. In their work, they proposed an LPPM for an LBS that take into account each user's service quality constraints. To evaluate the performance of the LPPM against these constraints, the authors of [35] used the service quality metric.

The works [23, 50] focused on obfuscation mechanisms. The first one studied methods of location obfuscation and provided solutions with improved results of utility. In the latter, the authors exploited the privacy level obtained with geo-indistinguishability, examined the trade-off between privacy and utility and provided an equivalent formal definition of ϵ-geo-indistinguishability as an adversary error.

Based on the previous works, utility can be defined as the expected quality loss of a mechanism [16, 35]. Formally, these works defined quality loss by the following equation:

$$Q(f, \mathbf{x}, \mathbf{z}) = \sum_{x \in \mathcal{X}, z \in \mathcal{Z}} f(x, z) d(x, z) \tag{2.6}$$

where $d(\cdot)$ is a quality loss metric, typically the Euclidean distance, since the degradation of LBSs can be quantified by the distance between the exact location x and the obfuscated location z.

Another quality loss metric is the squared Euclidean distance d^2 employed in [23]. This metric is typically used by applications that retrieve information in a certain area. For instance, considering an application that is used for finding Points of Interest (PoIs), when the obfuscation level increases, the Area of Retrieval (AOR) increases with the squared Euclidean distance between the exact user location x and the obfuscated location z. The AOR consists of the area over which the LBS retrieves the information (e.g. nearby PoI) to the user. Due to the fact that the AOR is centred at the obfuscated location z, this area must be such that it contains the Area of Interest (AOI) of the user. The AOI is centred at the exact user location and corresponds to the area over which the user wants to receive information from the LBS. Figure 2.8 shows an example of an AOI and an AOR, represented with a blue circle and a grey circle, respectively. From this figure, we have a user that intents to know the PoIs within 300 m. To do so, the user requests that information to the LBS within 1 km of the obfuscated location z. Thus, the AOI is contained in the AOR and the user receives the wanted information.

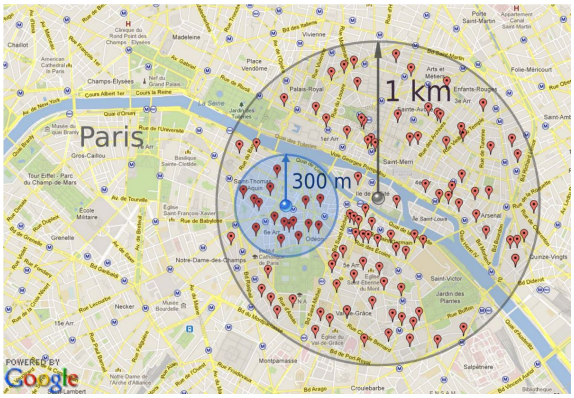


Figure 2.8: Example of an AOI of 300 m radius and an AOR of 1 km radius (from [22]).

The work [51] introduced the notion of (α, δ)-usefulness, which was used by the authors of geo-indistinguishability to measure its usefulness [22]. In this latter work, the authors stated that "A location perturbation mechanism K is (α, δ)-useful if for every location x the reported location $z = K(x)$ satisfies $d(x, z) \leq \alpha$ with probability at least δ.". From the perspective of the utility, a mechanism has a high utility level if the value of α is low and the value of β is high, since a lower value of α corresponds to a smaller distance between the exact user location x and the obfuscated location z.

In addition to the presented metrics, in the context of geo-indistinguishability, Oya *et al.* considered the average loss, $\bar{r}$, and the radius of the circular region centred around the true location x where the obfuscated location z can appear with probability 0.95, r_{95} [50]. In particular, for the Planar Laplace mechanism, given the parameter ϵ, the average loss is defined as follows: $\bar{r} = 2/\epsilon$. The radius r_{95} can be calculated using the Lambert W function as follows: $r_p = -\frac{1}{\epsilon}\left(W_{-1}\left(\frac{p-1}{e}\right) + 1\right)$, where p is the probability and W_{-1} is the negative branch of the Lambert W function.

2.3.3 Trade-off Between Privacy and Utility

Designing privacy-preserving mechanisms inherently corresponds to setting a trade-off between privacy and utility [14]. Specifically, in the case of obfuscation, the quality of the data is degraded before being collected by a service provider, which in turn results in a quality loss of the service. For example, reporting a location farther away from the exact location when retrieving the nearest restaurant, may result in getting the wrong restaurant.

Shokri *et al.* performed an analysis on the trade-off between the privacy level and the service quality loss [35]. As expected, they showed that a high level of privacy corresponds to a significant degradation of the service quality. Similar results were obtained by Krumm [33], where the author shows how much noise and quantization is necessary to preserve privacy against a realistic attacker.

The metrics presented in previous sections are the tools to measure the trade-off between privacy and utility. However, it should be clear that no widely accepted metric for both privacy and utility exists. In fact, multiple criteria should be taken into account [36], such as using complementary metrics (e.g. conditional entropy), specially due to the individual nature of privacy and personal privacy preferences [52].

Figure 2.9 shows an example of how the presented metrics can be used to measure the privacy and the utility level. The exact user locations $\mathbf{x}$ were obfuscated by an LPPM, producing the obfuscated locations $\mathbf{z}$, and the estimated locations $\hat{\mathbf{x}}$ were obtained by applying an attack. In this case, the privacy level can be measured by the estimation error and the utility error can be used as the quality loss metric. From this figure, we can also observe the trade-off between privacy and utility. Once we improve the privacy level, that is, increase the estimation error, we will degrade the utility of the LPPM.

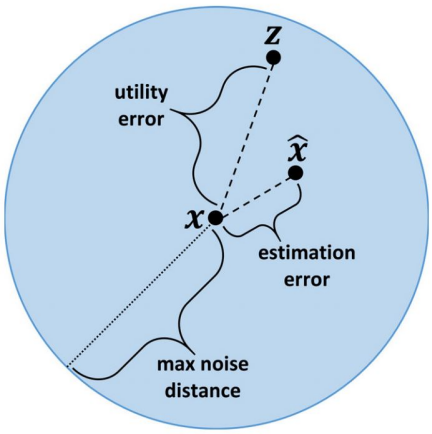


Figure 2.9: Privacy and utility errors (from [32]).

This page is intentionally left blank.

Chapter 3

Impact of Frequency of Reports on Location Privacy

After completing the study of the state of the art (see Chapter 2), we now evaluate how well the current techniques fare against the impact of the frequency of reports. To do so, we selected the techniques with the best performance and evaluated empirically against a dataset of real-world mobility data. The selection, analysis, and pre-processing of the dataset were done based on the location information needed for the state-of-the-art mechanisms. Furthermore, the pre-processing of the dataset included its sub-sampling, to produce different levels of frequency of updates for evaluation.

Briefly, our approach consisted in applying the implemented LPPM to the subsampled dataset, which resulted in a protected dataset. Then, the implemented attack is applied to the protected dataset to produce the adversary's estimation. Lastly, to assess the obtained results, we resort to suitable privacy and utility metrics.

This chapter describes the implementation of the selected LPPMs, the MM technique and corresponding attack, followed by the evaluation and the obtained results. The selected LPPMs were the PL [22] and the adaptive geo-indistinguishability [32] and the selected attacks were the MM proposed by Jagadeesh *et al.* [41] and an adaptation proposed by us to consider Laplacian noise instead of Gaussian noise. The PL mechanism was selected for the sporadic scenario, since it was the first mechanism that achieved the notion of geo-indistinguishability, which provides the formal privacy guarantees of differential privacy applied to location data. The adaptive geo-indistinguishability was selected for the continuous scenario, since it is a recent mechanism based on the PL that explores the correlation between reports for protecting location privacy. Regarding the attacks, since adversaries may use maps to locate the users [21], we selected a state-of-the-art MM [39], which enables us to locate vehicles on road networks. MM is usually applied for GPS navigation. To the best of our knowledge, this is the first time MM is considered for a tracking attack against location privacy.

3.1 Privacy Protection and Attack Mechanisms

This section describes in more detail the selected LPPMs (see Section 3.1.1) and the selected attack and an adaptation we have made (see Section 3.1.2).

3.1.1 Privacy Protection Mechanism

Generically, an LPPM is modeled as a probability distribution and can be denoted as [24]:

$$p(z_i|\mathbf{z}_{i-1}, \mathbf{x}_i) \tag{3.1}$$

where z_i is the obfuscated location and x_i is the exact user location. Thus, it means the probability of observing the obfuscated location z_i generated from location x_i.

This subsection details the implemented LPPMs, the PL geo-indistinguishability and the adaptive geo-indistinguishability. These mechanisms were developed for the sporadic scenario and the continuous scenario, respectively.

Geo-Indistinguishability

The geo-indistinguishable PL consists of adding 2-dimensional Laplacian noise centred at the exact user location x and with the following Laplacian distribution, whose probability density function (pdf) is:

$$p(z|x) = D_x(z) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d_{\mathrm{x}}(x,z)} \tag{3.2}$$

To obtain z from x using equation (3.2), we can add a randomly drawn vector expressed as a radius r and angle Θ. In this case, Θ is uniformly chosen from $[0, 2\pi)$ and r is computed by drawing p uniformly from $[0, 1)$ and feeding it to the inverse planar Laplacian cumulative distribution function. This function is calculated using the negative branch W_{-1} of the Lambert W function and is defined as:

$$C^{-1}(p) = -\frac{1}{\epsilon}\left(W_{-1}\left(\frac{p-1}{e}\right) + 1\right) \tag{3.3}$$

Therefore, the obfuscation location z is calculated by $z = x + \langle r\cos\Theta, r\sin\Theta\rangle$ and the Euclidean average quality loss achieved by this mechanism is $2/\epsilon$.

In our work, the PL is applied under multiple values of ϵ. The used set is defined as $\epsilon = [0.016, 0.032, 0.064, 0.128]$ m^{-1}.

Adaptive Geo-Indistinguishability

The adaptive geo-indistinguishability was proposed for continuous scenarios. This mechanism uses the PL with a dynamic ϵ that is computed according to the correlation between the new location and the past locations. Based on this correlation, the adaptive mechanism adjusts the amount of noise required to obfuscate the exact user location x. Thus, the mechanism increases the privacy level when the correlation between reports is high and improves the utility level when the correlation between reports is low. The correlation is measured as the error between an estimation and the exact user location, where the estimation is obtained using a simple linear regression. Formally, we can define the dynamic ϵ as follows [53]:

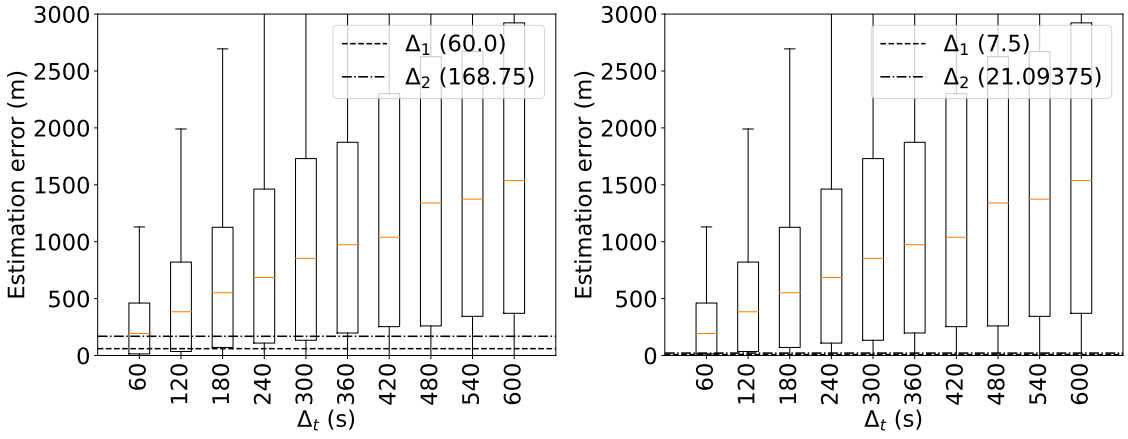
$$\epsilon = \begin{cases} \alpha \times \epsilon, & \text{if } d(x, \hat{x}) < \Delta_1 \\ \epsilon, & \text{if } \Delta_1 \leq d(x, \hat{x}) < \Delta_2 \\ \beta \times \epsilon, & \text{if } d(x, \hat{x}) \geq \Delta_2 \end{cases} \tag{3.4}$$

where x is the exact user location, $\hat{x}$ is the estimation, $d(\cdot)$ is the euclidean distance, Δ_1 and Δ_2 are two thresholds, and α and β are two constants. The authors also specify the following constraints: $\Delta_2 > \Delta_1$, $0 < \alpha < 1$, and $\beta > 1$. From the first branch of the equation (3.4), we have that if the distance between the exact user location and the estimation is lower than a small threshold Δ_1, i.e. high correlation, then privacy should be improved. To do so, ϵ is decreased by a factor $\alpha < 1$. On the other hand, when the error is larger than a higher threshold Δ_2, i.e. low correlation, the utility is enhanced by multiplying ϵ with the factor $\beta > 1$ (third branch). Otherwise, when the error is between $[\Delta_1, \Delta_2[$, the value of ϵ does not change. In Table 3.1 are presented the values defined for the parameters of the mechanism in the original work [32].

Parameter	Value
Δ_1	$0.96 \ / \ \epsilon$
Δ_2	$2.7 \ / \ \epsilon$
α	0.1
β	5

Table 3.1: Parameters of the adaptive mechanism from [32].

In our work, the adaptive mechanism is applied considering the values of ϵ that were used in the original PL mechanism. As parameters of the mechanism, we started by using the values defined in the original work. Figure 3.1 shows the boxplot of the estimation errors for the minimum and the maximum value of the used set of epsilon. From this figure, we can observe how the estimation errors are related to the thresholds Δ_1 and Δ_2 used in the original work. In particular, we can observe that the adaptive geo-indistinguishability is benefiting the utility instead of the privacy level for the majority of the values of ϵ and Δ_t, since most instanced appear above the Δ_2 threshold. In order to have diversity in the behaviour of the adaptive mechanism, we selected two different values of Δ_1 and Δ_2. Figure 3.2 shows the boxplot of the estimation errors with the selected thresholds, $\Delta_1 = 750$ and $\Delta_2 = 1750$. This ensures that we encompass a set of scenarios in which adaptive geo-indistinguishability optimises for privacy (lower values of Δ_t, where most instances are below Δ_1), utility (higher values of Δ_t) and intermediate cases. Lastly, regarding the simple linear regression, we chose to use the parrot function because it exhibited the best results [53]. The parrot function simply consists of returning the previous value as the prediction.



(a) $\epsilon = 0.016$ (b) $\epsilon = 0.128$

Figure 3.1: Boxplot of the estimation errors of the adaptive geo-indistinguishability for different values of epsilon ϵ, with varying minimum interval between points Δ_t. Dashed lines correspond to the thresholds Δ_1 and Δ_2 used in the original work [32].

3.1.2 Map-Matching

As mentioned before, we implemented two attacks, the original MM mechanism proposed in [41] and an adaptation proposed by us to consider Laplacian noise instead of Gaussian noise. Hereupon, the implementation of the mechanisms is described.

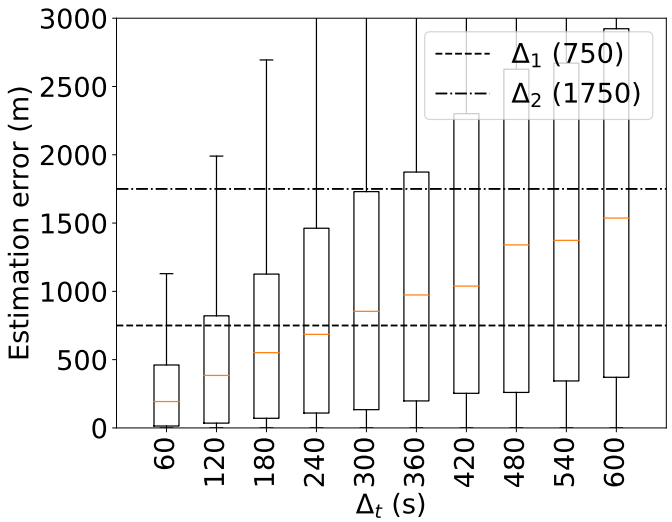


Figure 3.2: Boxplot of the estimation errors of the adaptive geo-indistinguishability for different values of epsilon ϵ, with varying minimum interval between points Δ_t. Dashed lines correspond to the thresholds Δ_1 and Δ_2 used in our work.

Let us denote the location report (referred as location observation or simply observation in [41]) at timestamp i as $o_i \in \mathcal{R}^2$. Although the report is not obfuscated, it is assumed to be noisy due to measurement errors. To apply the MM mechanism it is required a road network, which corresponds to a direct graph $G = (V, E)$, where V is a set of nodes representing intersections and endpoints of road segments and E is the set of these segments. A path p between nodes u and v is a sequence of edges $e_1, \ldots, e_n$ such that u is the start of e_1 and v is the end of e_n. Given a sequence of T noisy observations $o_1, \ldots, o_T$, the objective of a MM algorithm is to find a path p in G that corresponds to a sequence $o_{1:T}$. Towards this goal, in [41] a Hidden Markov Model (HMM) is used.

For each noisy observation o_i, the HMM's hidden states at time step i correspond to potential locations on the road where the user can be. The k^{th} potential location at time step i can be denoted as $s_{i,k}$ and the hidden true state can be denoted as $s_i^* = x_i$. Generally, the location measurement error, that is, the distance between the true state and the observed location, is assumed to follow a Gaussian distribution with zero mean [40, 41]. For a given state $s_{i,k}$, the probability of the observation o_i to occur is designated emission probability, which is defined as:

$$p(o_i|s_{i,k}) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{g(o_i,s_{i,k})^2}{2\sigma^2}} \tag{3.5}$$

where σ is the standard deviation of the measurement error and $g(o_i, s_{i,k})$ is the great-circle distance, that is, the shortest distance along the surface of the earth, between the observation o_i and the state $s_{i,k}$. From equation (3.5), it is possible to infer that closer states to the observation will have a higher probability than farther states.

The probability that the vehicle moves from state $s_{i-1,j}$ to $s_{i,k}$ is designated transition probability and depends on both the circuitousness of the path and on the temporal plausibility, that is, if the travelled distance is plausible given the time interval between timestamps $(t_i - t_{i-1})$. To measure the circuitousness of the path, the authors of [41] defined the following equation:

$$y(s_{i-1,j}, s_{i,k}) = \frac{d(s_{i-1,j}, s_{i,k}) - g(s_{i-1,j}, s_{i,k})}{(t_i - t_{i-1})} \tag{3.6}$$

where $g(s_{i-1,j}, s_{i,k})$ is the great circle distance between the states and $d(s_{i-1,j}, s_{i,k})$ is the

driving distance, which is the length of the minimum-travel-time path between $s_{i-1,j}$ and $s_{i,k}$ on the road network, calculated using Dijkstra's shortest path algorithm [54]. For the temporal plausibility, the equation is given as:

$$z(s_{i-1,j}, s_{i,k}) = \frac{\max\left(f(s_{i-1,j}, s_{i,k}) - (t_i - t_{i-1}), 0\right)}{(t_i - t_{i-1})} \tag{3.7}$$

where $f(s_{i-1,j}, s_{i,k})$ is the free-flow travel time, in seconds, of the optimal path between the states $s_{i-1,j}$ and $s_{i,k}$. Finally, the transition probability is defined as:

$$p(s_{i,k}|s_{i-1,j}) = \lambda_y e^{-\lambda_y y(s_{i-1,j}, s_{i,k})} \lambda_z e^{-\lambda_z z(s_{i-1,j}, s_{i,k})} \tag{3.8}$$

where λ_y and λ_z are empirically determined parameters from equations (3.6) and (3.7), respectively.

The most likely path from the HMM is computed using a Viterbi algorithm as follows:

$$\begin{aligned} V_{1,k} &= p(o_1|s_{1,k}) \\ V_{i,k} &= p(o_i|s_{i,k}) \max_j \left(V_{i-1,j} p(s_{i,k}|s_{i-1,j})\right) \end{aligned} \tag{3.9}$$

where $V_{i,k}$ corresponds to the joint probability of the most likely state sequence ending at state $s_{i,k}$ based on the observations $o_1, \ldots, o_i$. The index j that maximises $V_{i,k}$ is stored for each k as it points to the predecessor state $s_{i-1,j}$ that most likely leads to $s_{i,k}$. By saving the j's at each timestamp that maximise $V_{i,k}$, it is possible to obtain the most likely sequence for observations $o_1, \ldots, o_T$, starting in $\max_w V_{T,w}$. The path p is then obtained by concatenating the optimal (shortest) paths between consecutive states in the most likely sequence.

However, the optimal solution might not be obtained using the shortest segments to connect the states. In [41], an heuristic was provided that uses features to take into consideration drivers' preferences and thus increase the likelihood of getting the right segment between states. For this analysis, we will consider the shortest path as the optimal solution, thus we will omit the proposed route choice model. Furthermore, as shown in [41], the improvement obtained by the route choice model is less than 10%.

3.1.3 Map-Matching as an Attack to Location Privacy

MM can be used as a pre-processing technique in an LBS, where the location reports o_i are mapped to the most likely position for x_i, that is, $x_i = s_i^*$. Nevertheless, MM can also be used by an adversary to track/locate a user even if the latter is using an LPPM, as described below.

The existing MM mechanisms have considered Gaussian noise in location data readings, which has been proven effective for the measurement of noise from GPS or cellular network readings [40, 41]. The usage of an LPPM acts as a noisy channel described by equation (3.1). The implemented LPPM adds Laplacian noise instead of Gaussian noise. Therefore, we decided to adapt the MM method previously described to consider Laplacian noise as well. This adaptation is designated PLMM and solely consists in updating the emission probability defined in equation (3.5) to the following:

$$p(o_i|s_{i,k}) = p(z_i|s_{i,k}) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(s_{i,k}, z_i)} \tag{3.10}$$

Since the observation is now the obfuscated report ($o_i = z_i$), we replaced o_i for z_i. Intuitively, equation (3.10) is the probability of observing the obfuscated report z_i generated from position (hidden state) $s_{i,k}$.

To measure the obtained privacy, we can use the adversary error from equation (2.2) using z_i. However, for a tracking attack, a point-by-point metric would fail to assess the

effectiveness of the tracking, as the error could be 0 and the estimated trajectory could be different from the real trajectory. The authors of [41] define *F-score*, also called F_1 score, to evaluate the accuracy of the MM, which can be calculated by the following equations.

$$\begin{aligned} precision &= \frac{L_{correct}}{L_{matched}} \\ recall &= \frac{L_{correct}}{L_{truth}} \\ F_1 score &= 2 \times \frac{precision \times recall}{precision + recall} \end{aligned} \tag{3.11}$$

where $L_{matched}$ is the length of the output path, L_{truth} is the length of the corresponding ground-truth and $L_{correct}$ is the length of the portions of the output path that overlap with the ground-truth path. This metric basically measures how accurate the mechanism is through the amount of overlapped path, $L_{correct}$, between the adversary's estimated path, $L_{matched}$, and the ground-truth's path, L_{truth}. The value of F_1 score varies between 0 and 1. From the utility perspective of the MM technique, the worst case corresponds to F_1 score = 0 and the best case corresponds to F_1 score = 1. The best case occurs when both the precision and the recall are 1, that is, when the $L_{matched}$ is equal to the L_{truth} and, consequently, the $L_{correct}$ is equal to the L_{truth}. The worst case occurs when the $L_{matched}$ does not overlap the L_{truth}, which corresponds to $L_{correct} = 0$.

3.2 Evaluation

The following subsections describe the experimental setup, the methodology, and the results.

3.2.1 Experimental Setup

This subsection describes the experimental setup for the experiments, namely, the selected dataset and its pre-processing.

Dataset Selection

The choice of the dataset took into account the publicly available location datasets. Considering the selected mechanisms, the location data should either be reports made by vehicles or the dataset should have information about the method of transportation. Regarding the frequency of reports, since we want to perform an analysis in continuous scenarios, a dataset that allows downsampling is an important characteristic, that is, a dataset with high frequency of reports. Therefore, we briefly present three public datasets with the aforementioned characteristics:

- **Taxi Cabs in USA** [55] - constituted by more than 536 taxis travelling in the area of San Francisco, with duration of 30 days and update rate of about 10 seconds. Each report has information about the occupancy of the taxi cab;
- **Taxi Cabs in Rome, Italy** [56] - constituted by 306 taxis travelling in the area of Rome, duration 30 days and update rate of about 7 seconds;
- **GeoLife** [57] - constituted by 182 users worldwide, with duration of 3 years and variable update rate. It is divided by trajectories and it has reports from different transports.

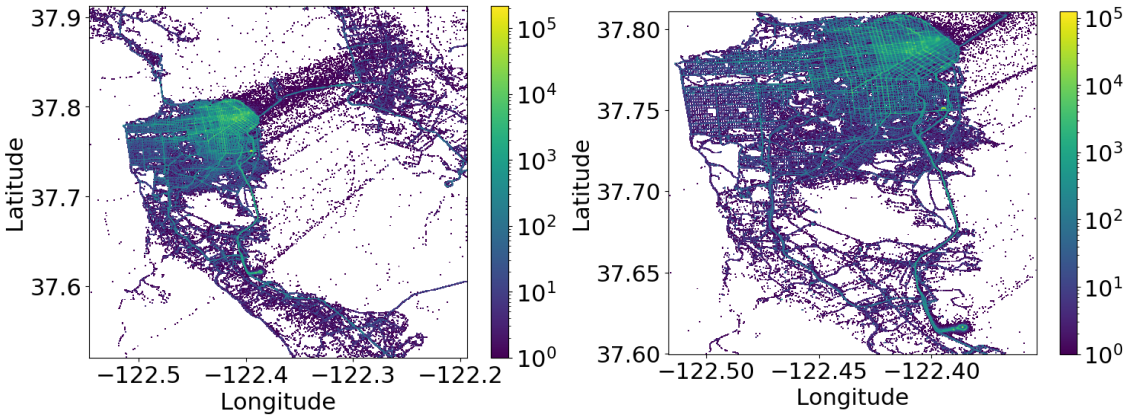
Since the selected attack is a road network MM mechanism, only vehicular trajectories can be considered. Based on the descriptions mentioned above and the performed analysis of the datasets, we selected the *Taxi Cabs in USA*, whose frequency of updates is high and the division into trajectories is possible through the occupancy of the taxi. The *GeoLife* dataset has variable update rate and has reports from different transports, thus it will not be considered for the experiments. On the other hand, the *Taxi Cabs in Rome* dataset does not have information about the occupancy of the taxi and, hence, it is harder to divide the data into trajectories.

The analysis performed to the datasets consisted in three main steps. The first step was the comparison of the time interval between samples, which allowed us to discard the *GeoLife* dataset due to the existing time gaps, that is, discontinuities in the reports along a trajectory. Hence, the second and third steps were made in the datasets of taxis. The second step consisted in checking the number of trajectories with and without passenger. While the *Taxi Cabs in USA* has a flag for the occupancy, the *Taxi Cabs in Rome* dataset has no information about it, which prevented us from dividing the data into trajectories in a trivial way. Therefore, after the analysis of the number of occupied versus free trajectories just for the *Taxi Cabs in USA*, we concluded that the number of trajectories with passengers was enough (464246 out of 928301) and we could discard the remaining ones. The third step consisted in checking the duration of trajectories, to evaluate if for different subsamples (e.g. over 6 minutes) there were enough points to consider, which was confirmed. The dataset is constituted by 1451 trajectories with a duration of at least 1 hour, that is, considering a trajectory with a duration of 1 hour and a subsample of 60 seconds, the trajectory is constituted by at least 60 points.

Dataset Pre-Processing

Since MM is computationally expensive, we started by selecting the relevant trajectories as following. We first limited the distribution of trajectories to the peninsula of San Francisco, as this is the most dense area as shown in Figure 3.3. Figure 3.4 shows this bounding box. Then we considered only trajectories with passengers, where the flag of occupancy is true [58]. This division allowed us to remove cases where the taxi was stopped waiting for a client. Finally, we selected trajectories with a duration of at least 1 hour, with intervals between reports of at most 100 seconds, to avoid temporal discontinuities between reports. This pre-processing resulted in 46 trajectories. To observe if the dataset contained noisy readings, we displayed the trajectories in the map and did a manual inspection of some of these trajectories, which confirmed our premise. Figure 3.5 gives an example where some GPS locations were reported in the ocean instead of in the bridge that the vehicle was clearly crossing.

To enhance the original data, we first apply the MM mechanism described in Section 3.1.2 to the 46 trajectories from the original dataset. Since we have no ground-truth and the MM [41] was applied to mobile network location data, the estimated noise standard deviation σ in [41] is considerably higher than in our dataset. Therefore, as we are unable to estimate σ, we use the parameters from [59], which is the baseline to the work in [41] and which uses GPS data as in our case. In [59] the estimated standard deviation was $\sigma = 6.86$m and they limited the potential locations $s_{i,k}$ to a bounding-box of 50m centred in the noisy GPS reading o_i. For the other parameters, we use the original values of [41]: $\lambda_y = 0.69$ and $\lambda_z = 13.35$. The constraint of the 50m radius around o_i produced observations without candidate points in 41 of the 46 trajectories due to the existing nodes of the road network. For these observations, we consider the nearest node of the road network as candidate. Moreover, after further manual inspection, we observed that in some of the trajectories the taxi stays roughly in the same place, which we attribute to heavy traffic. Consequently, we removed those trajectories and we obtained 30 trajectories as test data,



(a) Points over and around San Francisco

(b) Points over the peninsula of San Francisco

Figure 3.3: Distribution of the points of the dataset.

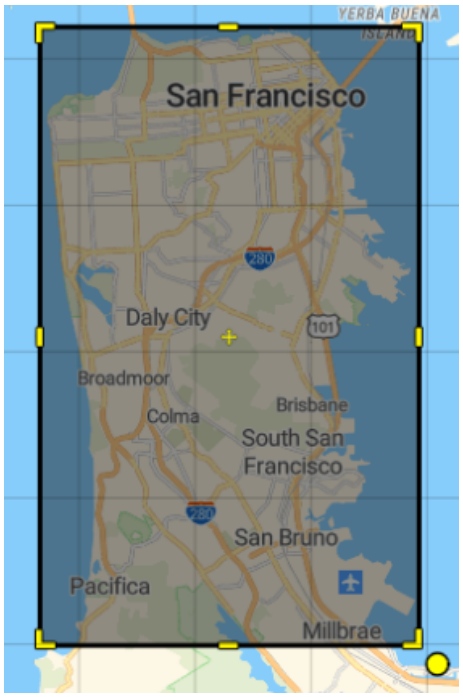


Figure 3.4: Bounding-box over the peninsula of San Francisco, defined from south and west by the coordinates (37.5996104427, -122.5168704724) and from north and east by the coordinates (37.81093499, -122.3535056708).

Figure 3.5: GPS locations reported with noise.

henceforth referred as our ground-truth.

Finally, to vary the frequency of reports we subsample the dataset by suppressing reports such that the interval between consecutive points is at least Δ_t. Since our focus was on continuous scenarios, we selected the following set of values from 60 to 600 seconds: $\Delta_t = [60, 120, 180, 240, 300, 360, 420, 480, 540, 600]$ seconds. It should be noticed that the values in our set are already considered low-sampling rate in the context of MM [39, 40]. In the selected MM technique [41], they consider a range of frequencies between 60 and 300 seconds.

3.2.2 Methodology

Figure 3.6 summarises the followed methodology. As explained in Section 3.2.1, the GPS data is pre-processed using the MM technique, resulting in the ground-truth, which in turn is subsampled considering the aforementioned values of Δ_t. Then the LPPM is applied to the subsampled data, i.e. to the exact locations, as explained in Section 3.1.1. Finally, both the original MM (MM) and the adapted MM (PLMM), which considers Laplacian noise (see Section 3.1.3), are executed on the obfuscated locations to obtain the adversary's estimations. To evaluate the privacy level of the LPPM, we used the average adversary error, P_{AE}, as a point-by-point metric, and the F_1 score from equation (3.11) as a trajectory metric. Moreover, we resort to the quality loss metric, Q, to evaluate the trade-off between the privacy and the utility of the LPPM.

The parameters σ, λ_y and λ_z for the MM attack were estimated following the proposal of the authors in [41]. To estimate the σ, i.e. the standard deviation of the location measurement errors, we first measured the error between each user location and the corresponding ground-truth location, using the great-circle distance $g(\cdot)$. Then, considering the set $\mathbf{g}_i$ constituted by the measurement errors and assuming that these errors are Guassian distributed with zero mean, we used the Median Absolute Deviation (MAD), which is a robust measure resilient to outliers, to calculate σ. Therefore, we calculated σ as follows: $\sigma = 1.4826\ median_i(\mathbf{g}_i)$. To estimate λ_y and λ_z, we measured the circuitousness and the temporal implausibility for a selected group of trajectories. Based on the obtained values, we calculated the exponential distribution for both the circuitousness and the temporal implausibility. The value of λ_y and λ_z correspond to the rate parameter of these distributions. Regarding the selection of the trajectories, the authors used the paths with duration between 1 and 5 minutes, resulting in 4828 trajectories with an average length of 2.6 km. In the same way, we used the trajectories with duration between 1 and 5 minutes that had at least 2 km of travelled distance, resulting in 6003 trajectories. The estimation of the parameters resulted in the following values: $\lambda_y \approx 0.07$ and $\lambda_z \approx 0.74$. In Appendix B, we describe the estimation of the parameters λ_y and λ_z and present the respective distributions.

Furthermore, considering the efficiency of the attack, we only take into account candidate points within a radius computed for both MM and PLMM. To compute this radius, we use the inverse distribution function of the Gaussian and Laplacian distributions, such that the circle centred at the observation contains the exact location with 90% probability. Intuitively, this corresponds to the case where the attacker computes the set of potential locations, where with 90% probability the exact location is in the set. When there is not a candidate within this radius, we consider the nearest node of the road network as candidate. The road network used covers the area defined by the bounding box represented in Figure 3.4 and was obtained from OpenStreetMap using the OSMnx tool [60]. The road network is in the form of a *networkx multidigraph*, which is manipulated using the NetworkX tool [61].

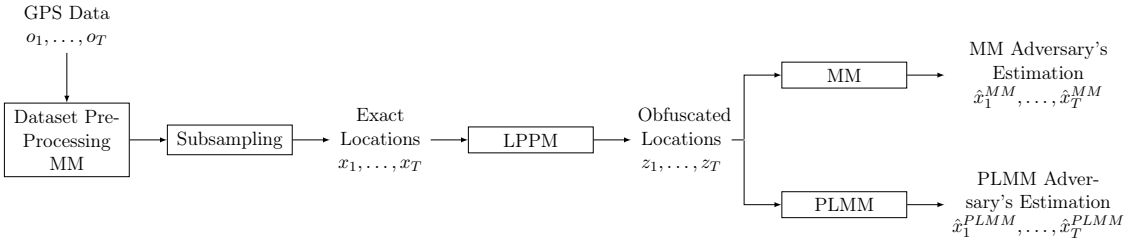
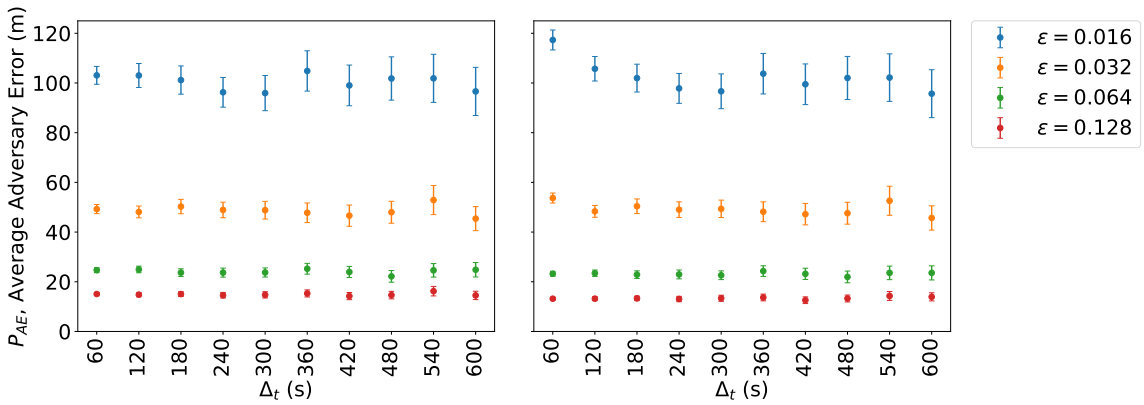


Figure 3.6: Diagram of the followed methodology.

3.2.3 Results

For our objective of evaluating of the impact of the frequency of reports on location privacy, we will present here the results for the PL mechanism only. The results for adaptive geo-indistinguishability, where epsilon is adjusted as function of the correlation between reports will be used as comparison against our proposed scheme in Chapter 4.

As aforementioned, a point-by-point metric to measure the adversary's estimation error is not suitable for tracking attacks. Moreover, such a metric does not reveal the effect of the frequency of the reports in both the MM and the PLMM, as shown in Figure 3.7, where the average adversary error, P_{AE}, is reasonably similar for all Δ_t. In fact, this can be explained because the adversary's estimation error considers only the distance between the exact location and the adversary's estimation, which is not influenced by the temporal correlation. Nevertheless, we can observe the effect of the obfuscation level. A higher ϵ corresponds to a lower radius of obfuscation and, hence, to a lower adversary's estimation error. Lastly, we can observe from Figure 3.7 that the results of the PLMM are identical to the results of the MM, with the maximum difference between both of approximately 15 m, for $\Delta_t = 60$ s.

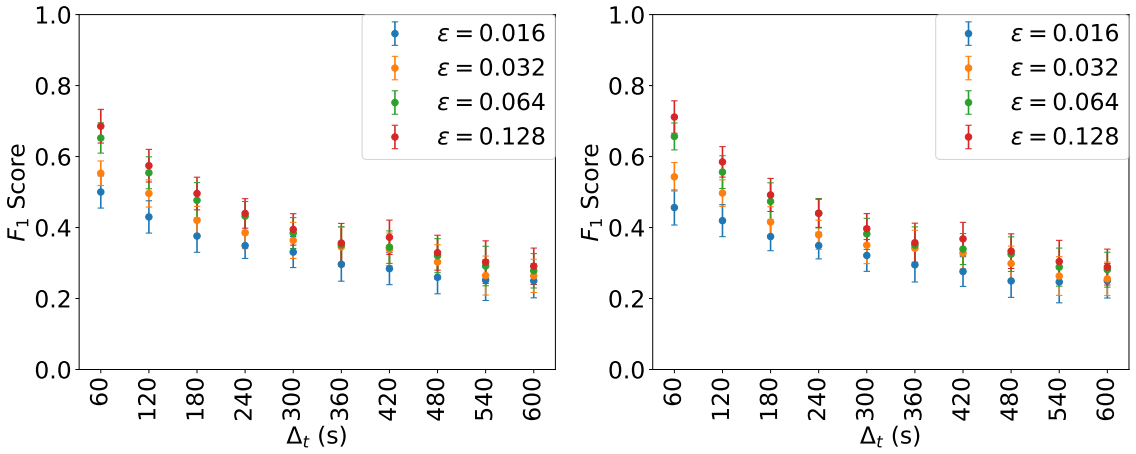


(a) MM (b) PLMM

Figure 3.7: Average adversary error of MM and PLMM for different values of geo-indistinguishability privacy parameter epsilon ϵ, with varying minimum interval between points Δ_t, and respective 95% confidence intervals.

In order to observe the impact of the Δ_t on tracking attacks, we used the metric proposed by the authors of [41], the F_1 score from equation (3.11). Figure 3.8 shows the effect of the correlation between reports on the MM attack and on the PLMM attack. From this figure, we can observe that the decrease of the frequency of reports (i.e. increased minimum interval Δ_t values) leads to a degradation of both the MM and the PLMM. In fact, as result of the decrease of the frequency of reports, the data become more sporadic and, consequently, the trajectories will match with less precision. These results corroborate

that the variations of the frequency of reporting do have an impact in the effectiveness of MM as a tracking attack.

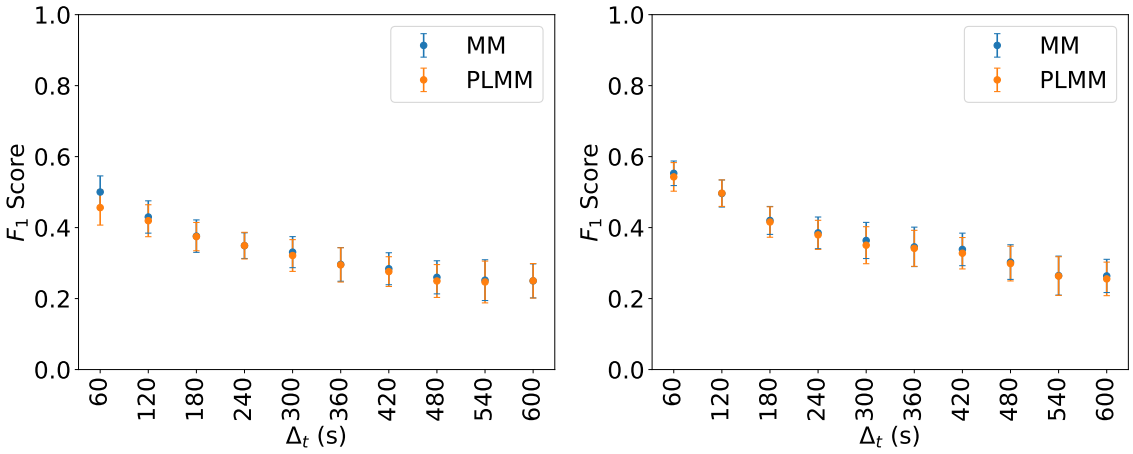


(a) MM (b) PLMM

Figure 3.8: F_1 score of MM and PLMM for different values of geo-indistinguishability privacy parameter epsilon ϵ, with varying minimum interval between points Δ_t, and respective 95% confidence intervals.

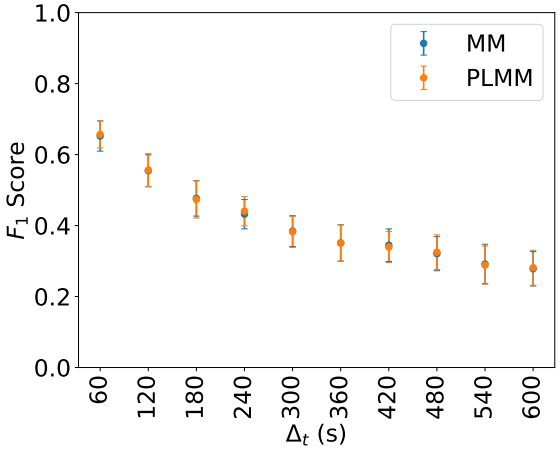
Regarding the adapted MM, Figure 3.9 shows the comparison between the MM and the proposed PLMM for selected values of ϵ, using the metric F_1 score. From this figure, we can observe that the adaptation PLMM has very similar results to the original MM, with minor differences in terms of F_1 score. This result reveals that the distribution used to add noise does not have a considerable impact on MM as a tracking attack and, therefore, in Chapter 4 we focus on the original MM only.

Finally, Figure 3.10 shows the privacy versus utility of MM and PLMM for different values of Δ_t, where each value of Δ_t is represented by a different colour. To assess the LPPMs performance, we measured the privacy and the utility through the average adversary error, P_{AE}, and the average quality loss, Q, respectively. For each value of ϵ, we calculated the average adversary error as function of the average quality loss, resulting in the pair (P_{AE}, Q), which is represented with a point in the figure. The dashed vertical lines correspond to the average value of epsilon at the empirical quality loss over all the values of Δ_t. For reference, the solid line corresponds to an adversary that uses the report as the estimation. From this figure, we observe that the curves for the different values of Δ_t are similar, which reveals again that a point-by-point metric fails to assess the impact of the frequency of updates on the privacy level. Moreover, these results show that there are some cases where using the attack gives an adversary's estimation more distant to the exact user location than the obfuscated point was. For instance, from Subfigure (a) of the Figure 3.10, we can observe that the obtained estimations for the $\epsilon = 0.128$ are above the solid line, which represents the obfuscated point. Therefore, this means that the distance between the estimations and the exact user location is bigger than the distance between the obfuscated location and the exact user location. In fact, when the attack matches the obfuscated point on the road, it makes the matched point closer to the obfuscation point, however, the matched point is not necessarily closer to the exact user location.

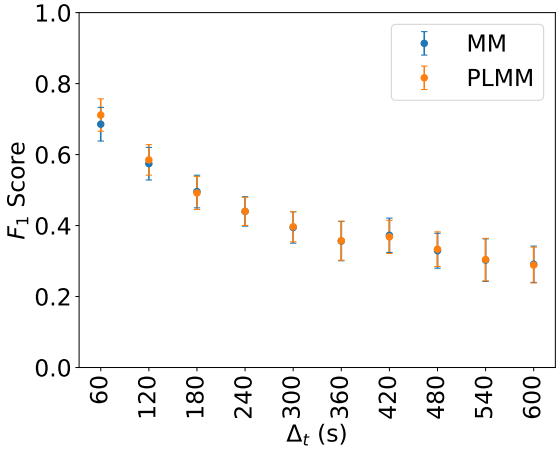


(a) $\epsilon = 0.016$

(b) $\epsilon = 0.032$

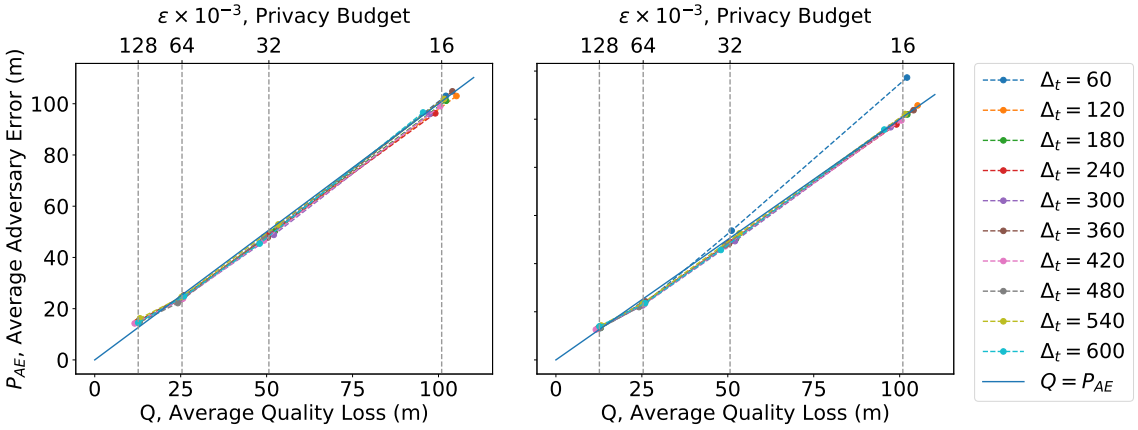


(c) $\epsilon = 0.064$



(d) $\epsilon = 0.128$

Figure 3.9: F_1 score comparison between the MM and the PLMM for different values of geo-indistinguishability privacy parameter epsilon ϵ, with varying minimum interval between points Δ_t, and respective 95% confidence intervals.



(a) MM (b) PLMM

Figure 3.10: Privacy versus utility of MM and PLMM for different values of Δ_t, where each value of Δ_t corresponds to a different colour. The points represent the pair (P_{AE}, Q), which is obtained for each value of ϵ. Dashed vertical lines are the average value of epsilon at the empirical quality loss over all the values of Δ_t. For reference, the solid line corresponds to an adversary that uses the report as the estimation.

Chapter 4

Clustering Approach to Location Privacy

In this chapter we propose a new location privacy-enhancing mechanism that considers the frequency of updates and geo-temporal correlations. In order to implement a protection mechanism against these intrinsic correlations of data, we took into consideration the approaches previously discussed in the state of the art (see Chapter 2). We started by looking at the implemented LPPM - PL - and took advantage of it for the sporadic scenario. Targeting the continuous scenario as well, we focused on the distance between the reports, which is influenced by the frequency of updates. Since a higher frequency of updates (i.e. a lower time interval between the reports) corresponds to a lower distance between the reports and to closer locations, our mechanism creates obfuscation clusters to protect those locations, as we will explain in this chapter.

We start by describing the development and implementation of the new LPPM, followed by the performed analysis and the obtained results. The evaluation of the developed mechanism considered the privacy level and the utility of the obtained data. This evaluation was performed based on the appropriate metrics, which were presented in Chapter 2. To assess the utility of the mechanism, we considered the application of the mechanism in a real use-case. Moreover, we compared our mechanism with existing mechanisms from the literature. For the sporadic scenario, we compare against the original PL mechanism, while for the continuous scenario, we assess against the adaptive geo-indistinguishability mechanism, which was also developed for continuous scenarios.

4.1 Clustering Geo-Indistinguishability

In order to develop a new mechanism that can be used both in the sporadic scenario and in the continuous scenario, we started by looking at the implemented geo-indistinguishable LPPM - PL, which is considered the state-of-the-art LPPM for the sporadic scenario. From the PL mechanism, we know that the exact user location x is reported as an obfuscated location z, which is obtained by adding 2-dimensional Laplacian noise centred at the exact user location. As we observed in the Chapter 3, the frequency of updates has impact on the privacy preservation of the user location. Taking these notions into consideration, our idea consists in creating a mechanism that obfuscates the exact user location x by applying the PL mechanism. Then, an obfuscation cluster centred at the real location x is created, such that the same obfuscated location z is reported for every real location inside the cluster. With this approach, we take advantage of the original PL for sporadic scenarios (i.e. low sampling frequency and distant reports), while providing a solution that leads to the same obfuscated report for continuous scenarios, in which real locations are close by.

Therefore, our mechanism produces an obfuscated location z_i within a certain radius

of obfuscation r for the first user location x_i, by directly applying the PL mechanism. The location x_i creates an obfuscation cluster centred at $x_c = x_i$, that is, a circle centred at x_c, whose obfuscated point is z_i. For the next user location x_{i+1}, the mechanism verifies if it is inside the area of the previous obfuscation cluster centred at x_c. If the user location is inside the area, the mechanism reports the previous obfuscated point, that is, $z_{i+1} = z_i$. Otherwise, the LPPM obfuscates the location x_{i+1} with the PL mechanism and creates a new obfuscation cluster centred at $x_c = x_{i+1}$. In order to verify if the user location is inside the area of the previous cluster, the mechanism calculates the distance d between the current location and the location that originated the previous cluster x_c, using the great circle distance $g(\cdot)$. The parameters of our scheme are then the radius of the obfuscation cluster and the value of the privacy parameter ϵ. To reduce the number of parameters, which in turn increases the usability of the mechanism, one can set r to depend on the ϵ value.

Figure 4.1 presents an example of our approach, which will be explained starting from subfigure (a) to subfigure (f). For the first user location x_1, our mechanism produces an obfuscated location z_1 within a certain radius of obfuscation r, by directly applying the PL mechanism. That obfuscation area centred at x_1 constitutes an obfuscation cluster centred at $x_c = x_1$. To simplify the description of the example, we will use x_i instead of x_c to represent each location that originates a cluster, where i is the timestamp. For the next user location x_2, the mechanism calculates the distance d between the new user location x_2 and the centre of the previous cluster x_1. Then, the mechanism verifies if it is inside the previous cluster or not. As we can observe in the subfigure (b), the distance between x_1 and x_2 is smaller than r, which means that the user location is inside the obfuscation cluster of x_1. Thus, our mechanism returns the obfuscated point z_2, which is equal to the previous obfuscated point z_1. In the same way, for the user location x_3, the distance between x_1 and x_3 is calculated. As we can observe in subfigure (c), the distance d is smaller than r and, consequently, the mechanism reports the point z_3, which is equal to z_1. For the user location x_4, we can observe in subfigure (d) that the distance d is bigger than the radius r and, consequently, the mechanism produces a new obfuscated point z_4, by applying the PL mechanism as shown in subfigure (e). Finally, subfigure (f) shows the reported obfuscated points z_1, z_2, z_3 and z_4 for the user locations x_1, x_2, x_3 and x_4, where z_1, z_2 and z_3 correspond to the same obfuscated point, due to our clustering mechanism.

Algorithm 1 shows the implemented approach. The parameters of the algorithm are the exact user location x_i, the privacy parameter ϵ and the radius of obfuscation r. By applying this algorithm, the user location x_i will be obfuscated and the algorithm will return the obfuscated location z_i. Regarding the parameters, the value of ϵ will be used to apply the PL mechanism and the radius r will be used to compute the radius of the obfuscation area of the clusters as explained above.

4.1.1 Privacy Analysis

As we observed in Chapter 3, the correlation between reports may degrade the privacy level of the LPPMs. In particular, when a user reports several nearby points, the PL mechanism leads to the disclosure of the user's information. For instance, if we consider the most continuous scenario possible, i.e. when the user is continuously reporting the same location, the PL mechanism will produce obfuscated locations for that user location, as shown in Figure 4.2. From the obfuscated locations and considering the behaviour of the Laplacian distribution used by the mechanism, we can delineate the centre of the obfuscation area, which enables us to discover the exact user location. Our proposed mechanism prevents this situation, since the clustering mechanism reports the same obfuscated point for nearby locations, which is a clear advantage of our mechanism.

Regarding the nearby locations, by the definition of ϵ-geo-indistinguishability, if the

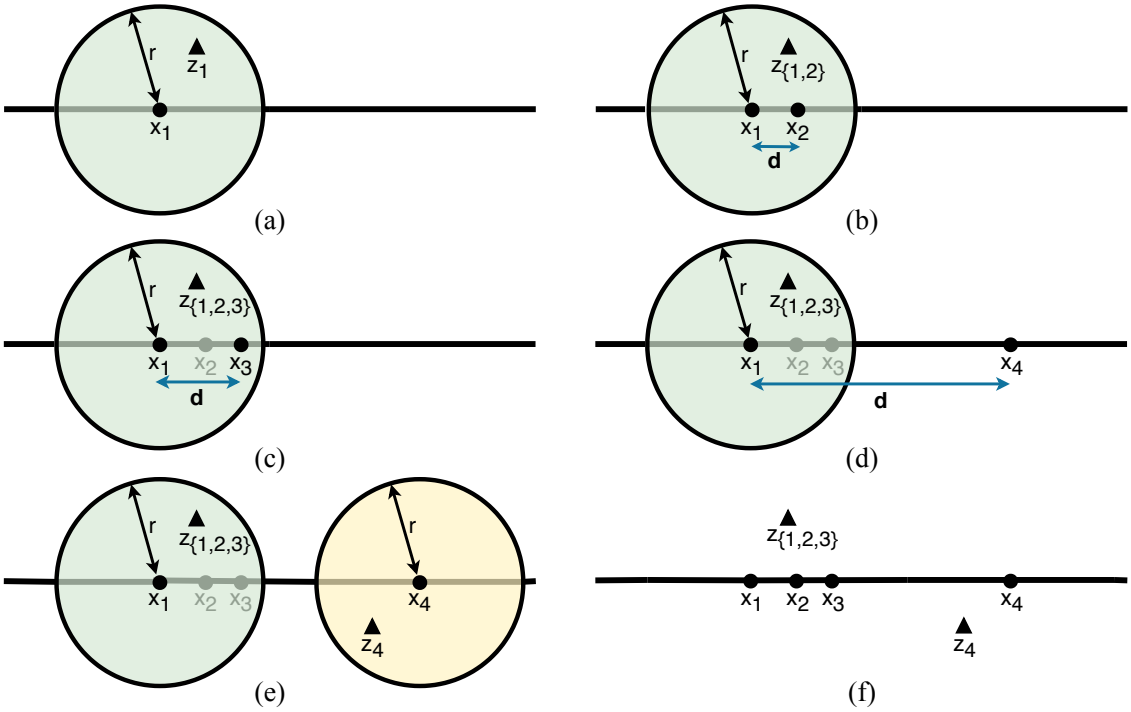


Figure 4.1: Example of the clustering geo-indistinguishability mechanism.

Algorithm 1 LPPM based on clustering

```
1:  function CLUSTERING(x_i, ε, r)
2:      if first report then
3:          x_c = x_i
4:          z_i = planarLaplace(x_i, ε)
5:      else:
6:          distance = g(x_c, x_i)
7:          if distance ≤ r then
8:              z_i = z_{i−1}
9:          else
10:             x_c = x_i
11:             z_i = planarLaplace(x_i, ε)
12:     return z_i
```

distance between two locations x, x' is at most r, where r is the radius of obfuscation, then the multiplicative distance between the distributions of x, x' is at most l, where l is the level of privacy (c.f. equation (2.5)). Thus, for closer locations, the distributions are similar and, consequently, the probability of generating the same obfuscated location is higher. Since our mechanism uses the same obfuscated point for locations that dist at most r, it is guaranteed that the obfuscated locations reported by the proposed mechanism are geo-indistinguishable, thus avoiding the need to use PL to produce a new obfuscated location.

Furthermore, the privacy level of the geo-indistinguishability scales linearly with the number of queries n [22]. Considering a mechanism K that is applied to a single query and a mechanism K' that is applied to n queries, if the mechanism K satisfies ϵ-geo-indistinguishably, then the mechanism K' will satisfy $n\epsilon$-geo-indistinguishability, due to its scalability. Therefore, since the mechanism applies geo-indistinguishability to each point independently, the privacy degradation increases with the increasing number of queries, because $n \times \epsilon$ grows. Each time the proposed mechanism uses the previous obfuscated location, it avoids a new application of the PL to produce a new obfuscated location. Therefore, our mechanism prevents the privacy degradation of the geo-indistinguishability that comes from multiple applications of the protection mechanism.

Lastly, although the number of reported points does not decrease, as a result of applying our mechanism, the reported point does not change in some of the cases, as shown in the example of Figure 4.1. In fact, once the user reports the same location instead of a new location, for the service, the user stays in the same location. Thus, there is less disclosure of user's information. Furthermore, since frequency of updates greatly impacts the distance between reports, our clustering mechanism takes advantage of the effect of the frequency of updates on the number of nearby points that require obfuscation.

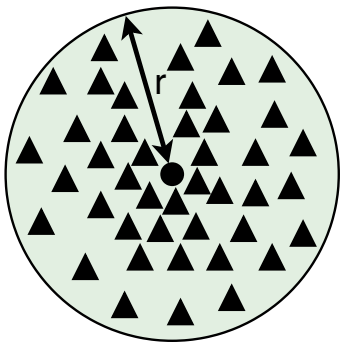


Figure 4.2: Example of multiple obfuscations from PL mechanism for the same user location within a radius r. The ● represents the exact user location and the ▲ represents the obfuscated locations.

4.2 Evaluation

The following subsections describe the performance of the proposed clustering geo-indistinguishability mechanism and evaluate the levels of privacy and the utility obtained. Moreover, we present the comparison between our mechanism and two existing mechanisms, the PL and the adaptive geo-indistinguishability.

In order to evaluate the performance of the clustering geo-indistinguishability, we used the methodology presented in Section 3.2.2 for the original MM using the same mobility dataset. The clustering mechanism was applied under multiple values of ϵ, using the previous set that was defined as $\epsilon = [0.016, 0.032, 0.064, 0.128]$ m^{-1}. To compute the

obfuscation radius r, we resorted to the original definition of PL, such that $\epsilon = \frac{l}{r}$ or, likewise, $r = \frac{l}{\epsilon}$. For that, we considered the above set of ϵ values and $l = log(4)$, as suggested by the authors [22]. As we can observe, the same value of r can be obtained with different combinations of values of ϵ and l. Therefore, the degrees of freedom of our mechanism actually correspond to the value of ϵ and r, being that r is a function of epsilon. As such, we focus our analysis on the effect of epsilon.

4.2.1 Number of Points per Cluster

Figure 4.3 shows the average of points per cluster obtained by applying clustering geo-indistinguishability as a function of Δ_t for various epsilon values. As aforementioned, the clusters were created according to the obfuscation radius, that is related to the value of ϵ. Thus, for the set of epsilon values, the used set of radiuses is approximately $r = [86.64, 43.32, 21.66, 10.83]$ m. As expected, for lower values of Δ_t, the number of points per cluster is higher than for higher values of Δ_t. This can be explained by the proximity of the locations when the time interval is lower. In particular, from this figure, we can observe that the number of points per cluster is approximately less than three for the values of $\Delta_t \geq 360$ s in all values of ϵ that we used. The other five values of Δ_t correspond to time intervals between 60 to 300 seconds, that is, from the case where the user is reporting at every minute until the case where the user is reporting every 5 minutes. Therefore, as we will detail in the following subsections, the impact of our mechanism on privacy and utility will be higher for values of $\Delta_t \leq 300$ s, that is, for time intervals smaller or equal than 5 minutes.

Furthermore, we can observe from Figure 4.3 that the average of points per cluster increases with the decrease of the ϵ value, for all Δ_t values. This can be explained by the original definition of PL, such that $\epsilon = \frac{l}{r}$ and, likewise, $r = \frac{l}{\epsilon}$. From this definition, we have that a higher value of ϵ corresponds to a smaller radius r. Thus, the radius of the obfuscation clusters is smaller for higher values of ϵ and, consequently, there are less points per cluster for those ϵ values.

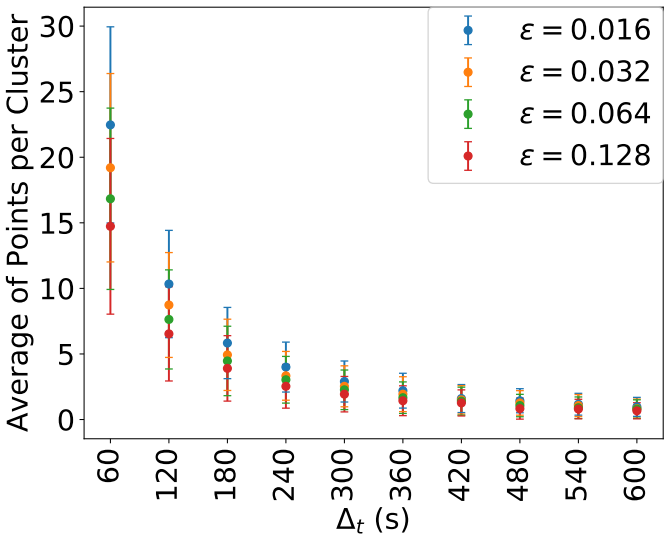


Figure 4.3: Average of points per cluster obtained by applying the clustering geo-indistinguishability for different values of epsilon ϵ, with varying minimum interval between points Δ_t, and respective 95% confidence intervals.

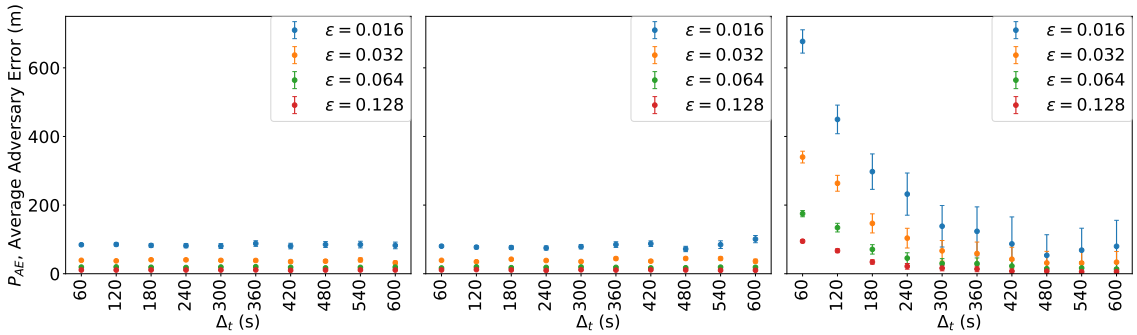
4.2.2 Privacy Evaluation

To evaluate the privacy of the mechanism, we used the adversary error as a point-by-point metric, and the F_1 score as a trajectory metric. The obtained results will be compared with the results of the PL and the adaptive geo-indistinguishability.

Adversary Error Metric

Figure 4.4 presents the average adversary error of the three mechanisms as a function of Δ_t for various epsilon values. As we can observe, the results of the clustering geo-indistinguishability are similar to the results of the PL mechanism. In fact, these results reveal that our mechanism maintains the privacy level point-by-point.

When we compare the results of the adaptive geo-indistinguishability with the results of the clustering geo-indistinguishability, we observe that the difference between the average adversary error is less than ∼10 m for $\epsilon = [0.016, 0.032]$ and $\Delta_t \geq 420$ s, for $\epsilon = 0.064$ and $\Delta_t \geq 300$ s, and for $\epsilon = 0.128$ and $\Delta_t \geq 240$ s. For the remaining cases, the adaptive geo-indistinguishability has a bigger adversary error, which can be explained by the fact that the adaptive mechanism is mostly benefiting the privacy level in those cases. As mentioned in Section 3.1.1, this behaviour is a consequence of the parameters used in the adaptive mechanism. From equation (3.4) and from Figure 3.2, we have that: $\epsilon = \beta \times \epsilon$ when the estimation errors are greater than Δ_2; $\epsilon = \epsilon$ when the estimation errors are between Δ_1 and Δ_2; and $\epsilon = \alpha \times \epsilon$ when the estimation errors are lower than Δ_1. Therefore, as we can observe in Figure 3.2, the majority of the estimation errors for values of $\Delta_t \leq 240$ s is lower than Δ_1, then the mechanism improves the privacy level by increasing the obfuscation level, which results in larger adversary errors. For the remaining values of Δ_t, the mechanism does not change the value of ϵ or improves the utility, by increasing the value of ϵ, which results in lower values of adversary error.



(a) PL (b) Clustering (c) Adaptive

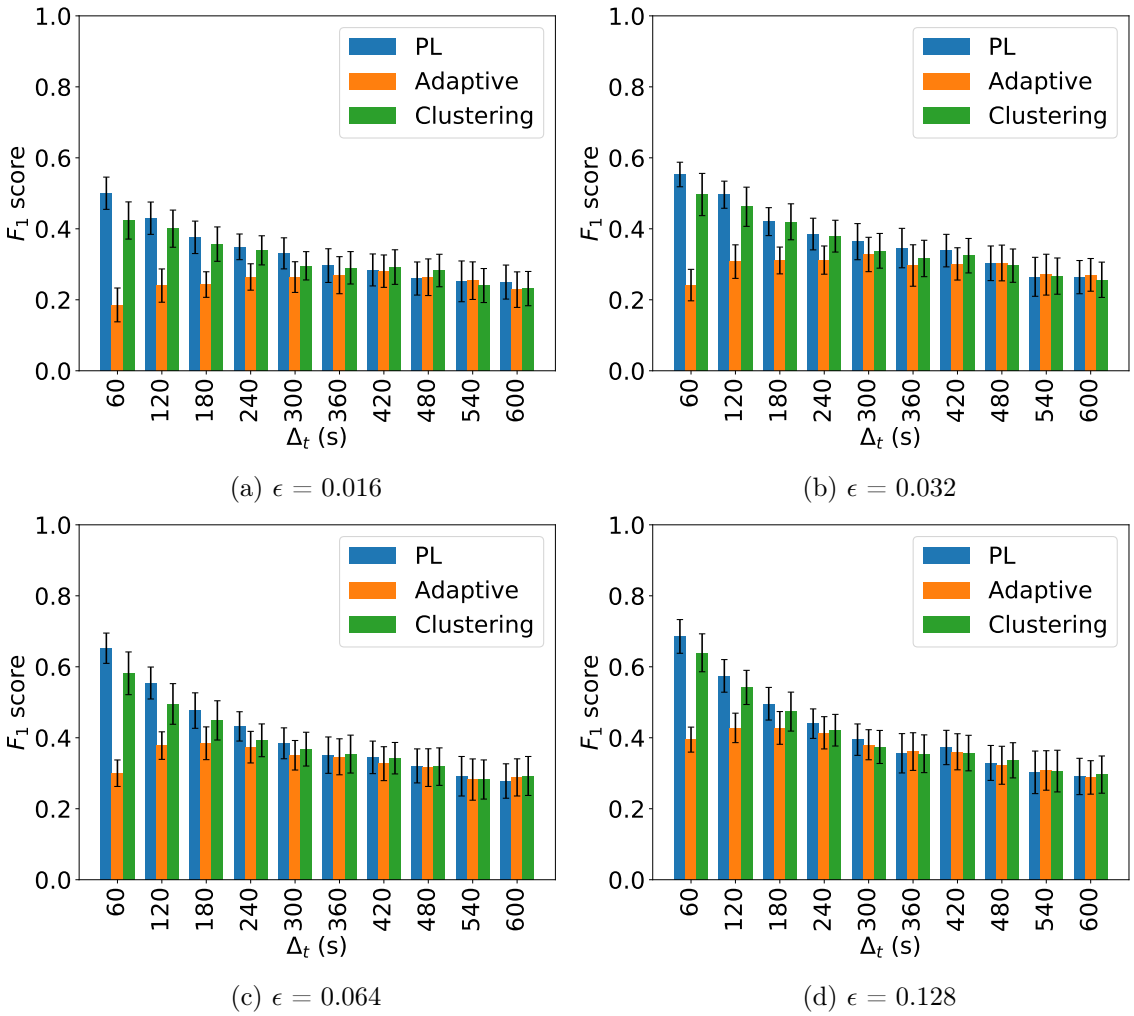
Figure 4.4: Average adversary error and respective 95% confidence intervals of PL, clustering and adaptive mechanisms for different values of geo-indistinguishability privacy parameter epsilon ϵ, with varying minimum interval between points Δ_t.

F_1 Score Metric

Figure 4.5 shows the comparison between the three mechanisms. When we compare the clustering geo-indistinguishability with the PL mechanism, we can observe that the clustering mechanism has lower values of F_1 score for all values of $\Delta_t < 360$ s and all values of ϵ, which means higher privacy level. For the remaining values of Δ_t, F_1 score is lower in some values of Δ_t and ϵ and slightly higher in others. As we showed in Section 4.2.1, the number of points per cluster is higher for $\Delta_t < 360$ s and, therefore, the impact of our mechanism is more significant for these values of Δ_t.

Regarding the adaptive geo-indistinguishability, we can observe that the results of the F_1 score become similar to the results of the clustering geo-indistinguishability with the increase of the Δ_t values, which can be explained by the behaviour of the adaptive mechanism. Since for higher values of Δ_t, the estimation errors are higher and, consequently, the mechanism tends to improve the utility of the data. Moreover, the difference between the F_1 score of the adaptive and the clustering mechanisms is less than $\sim 5\%$ for $\epsilon = [0.016, 0.032]$ and $\Delta_t \geq 300$ s, and for $\epsilon = [0.064, 0.128]$ and $\Delta_t \geq 240$ s. From Figure 4.5, we can further observe that the clustering geo-indistinguishability has lower values of F_1 score in some of these cases.

Lastly, we can observe from Figure 4.5 that for lower values of Δ_t and epsilon, the adaptive mechanism has an F_1 score of about 20%. Recalling the meaning of this metric, this value translates to an overlap between the output path and the ground-truth path of approximately 20%. Thus, the mechanism discloses less than a quarter of the original trajectory. While this is advantageous from a privacy perspective, it leads to a severe degradation of utility as we will now show.



(a) $\epsilon = 0.016$ (b) $\epsilon = 0.032$

(c) $\epsilon = 0.064$ (d) $\epsilon = 0.128$

Figure 4.5: Comparison between the F_1 score value of the PL, the adaptive geo-indistinguishability and the clustering geo-indistinguishability for different values of epsilon ϵ, with varying minimum interval between points Δ_t, and respective 95% confidence intervals.

4.2.3 Utility Evaluation

To evaluate the utility of the mechanisms, we consider a real use-case based on geofencing. Geofencing is the process of generating virtual geographical perimeters/areas in where events occur when users enter or leave such perimeters. A location service provider can create geofences around locations of interest (e.g. PoIs) as shown in Figure 4.6, such that users traversing the geofence can receive relevant information with respect to the location (e.g. marketing or discounts from supermarkets).

Therefore, we created geofences to several PoIs from San Francisco. In order to have diversity of PoIs, we used PoIs from different domains, namely: hotels, museums and supermarkets. These PoIs were obtained from OpenStreetMap using the OSMnx tool [60], resulting in a total of 524 PoIs. Figure 4.7 shows the distribution of the PoIs over the Peninsula of San Francisco. Moreover, the geofences were created under multiple values of radius r. The used set was defined as $r = [100, 200, 300, 500, 1000]$ m. This set was chosen according to the guidelines for creating geofences for android developers [62], where a minimum radius of 100-150 m is recommended.

In our work, when a user enters in the area of a geofence, the application retrieves this PoI. Thus, we executed the application for the ground-truth user mobility locations to obtain the ground-truth PoIs. Then, we executed the application for the obfuscated user mobility locations that result from applying the PL, the adaptive geo-indistinguishability and the clustering geo-indistinguishability, to obtain the reported PoIs. Finally, in order to measure how the reported PoIs match the ground-truth PoIs, we used the classification true/false positive/negative. Generically, this classification is defined as follows:

- A True Positive (TP) is an outcome where the positive class is predicted correctly by the model;
- A True Negative (TN) is an outcome where the negative class is predicted correctly by the model;
- A False Positive (FP) is an outcome where the positive class is predicted incorrectly by the model;
- A False Negative (FN) is an outcome where the negative class is predicted incorrectly by the model;

To classify the results as TP, TN, FP or FN, we first defined the positive class and the negative class. Since the objective of the application is to return PoIs, we define returning a PoI as the positive class and returning *None* as the negative class. When the reported PoI is equal to the ground-truth PoI, we have a TP. When both the ground-truth and the reported do not return any PoI, we have a TN. When the ground-truth returns a PoI or *None* and the reported returns a different PoI, we have an FP. Lastly, when the reported returns *None* and the ground-truth returned a PoI, we have an FN. This classification is summarised in Table 4.1.

Based on this classification, we were interested in knowing how many PoIs were correctly or incorrectly identified. To do so, we used the True Positive Rate (TPR) and the False Positive Rate (FPR), which are defined as follows:

$$\begin{aligned} TPR &= \frac{TP}{TP + FN} \\ FPR &= \frac{FP}{FP + TN} \end{aligned} \tag{4.1}$$

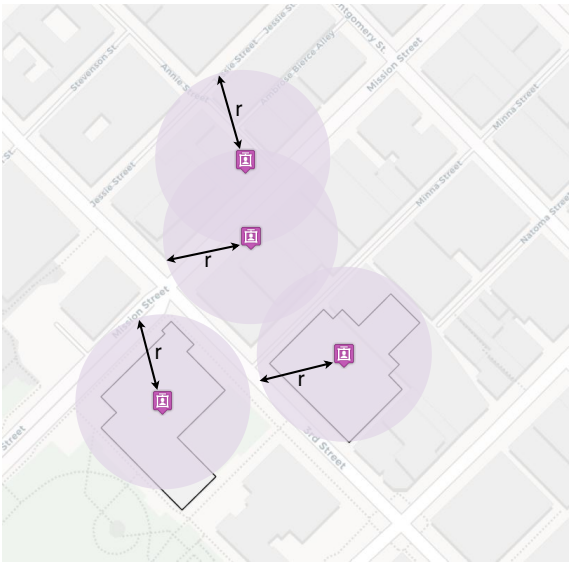


Figure 4.6: Example of geofences centred at the PoIs with a radius r.

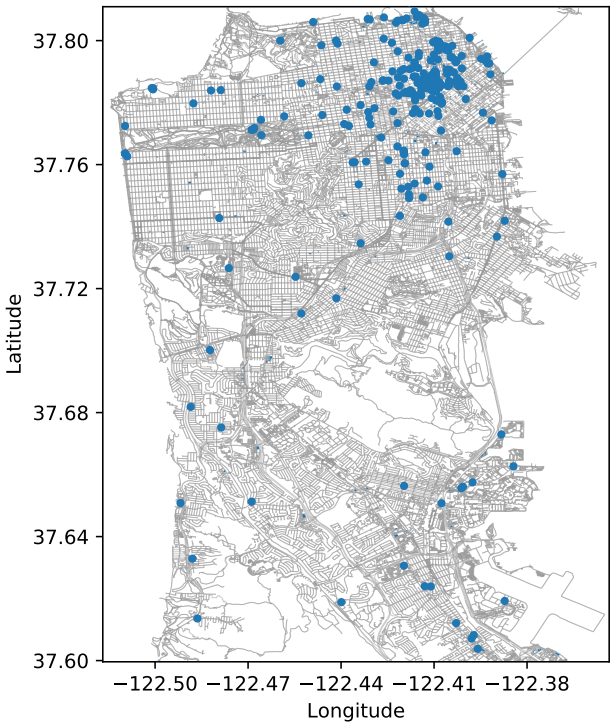


Figure 4.7: Distribution of the selected PoIs in San Francisco. Each blue point represents a PoI. The represented PoIs are hotels, museums and supermarkets.

Ground-Truth	Reported	Classification
A given PoI	Correct PoI	True Positive
None	None	True Negative
A given PoI, None	Incorrect PoI	False Positive
A given PoI	None	False Negative

Table 4.1: Classification True/False Positive/Negative.

Although we used the TPR and FPR, we could have used the True Negative Rate (TNR) and the False Negative Rate (FNR) because the metrics are complementary. However, from the point of view of the utility, the TPR is more relevant since it corresponds to the cases of both the ground-truth and the LPPM returning the same PoI.

Figures 4.8 and 4.9 respectively represent the TPR and the FPR of the three mechanisms. Based on the performed analysis between the values of both the TPR and the FPR for each value of Δ_t, ϵ and geofence radius and the average for the all values of Δ_t, we observed that they have similar behaviours. Therefore, we will present the figures with the average of both the TPR and the FPR for all values of Δ_t, for each ϵ, and for each geofence radius.

From Figure 4.8, we can observe that the TPR of all three mechanisms improves for growing epsilon values. This is expected since higher epsilon values correspond to lower obfuscation and, therefore, obfuscated locations that are closer to the real ones. This effect of epsilon fades away with increasing geofence radius, since a larger radius increases the size of the geofence region and, consequently, benefits the probability of getting the correct PoI, irrespectively of the level of obfuscation applied.

Regarding the comparison between the mechanisms, we can observe that the adaptive geo-indistinguishability has the lowest TPR for all values of ϵ and all values of the geofence radius. As we observed before, the adaptive mechanism has higher adversary errors, which means a higher distance between the reported point and the exact user location. Thus, these results reveal that the adaptive mechanism is improving the privacy level by degrading the utility of the data. On the other hand, the clustering geo-indistinguishability has the highest TPR, except for the radius of the geofence 100 m and $\epsilon = 0.016$. This exception can be explained because the $\epsilon = 0.016$ corresponds to an obfuscation radius of approximately 86 m. Thus, as the mechanism creates obfuscation clusters within a radius of 86 m, the distance between the obfuscated locations and the exact user locations included in the cluster can be higher than the radius of the geofence and, hence, the mechanism reports an incorrect PoI. As we mentioned before, when the geofence radius increases, the difference between the TPR of the clustering geo-indistinguishability and the other mechanisms decreases. In particular, when the radius of the geofence is 1 km, the TPR of the three mechanisms is similar for high values of ϵ, since the increase of the radius of the geofence, i.e. the increase of the geofence region, benefits the probability of reporting correct PoIs.

Figure 4.9 shows the FPR of the three mechanisms. Inversely to the TPR, here the FPR decays with increasing epsilon, since higher epsilon values correspond to less obfuscation and, therefore, improved FPR. As we can observe, the adaptive mechanism has the highest value for all geofence radiuses, which means that this mechanism reports more incorrect PoIs. On the other hand, the PL mechanism and the clustering geo-indistinguishability report fewer incorrect PoIs, again with our scheme closely following PL. Lastly, as aforementioned, when the radius of the geofence grows, the size of the geofence region increases

and, consequently, the probability of reporting PoIs is higher. However, this also leads to a high probability of reporting incorrect PoIs, which explains the increase of the FPR for larger geofence radius.

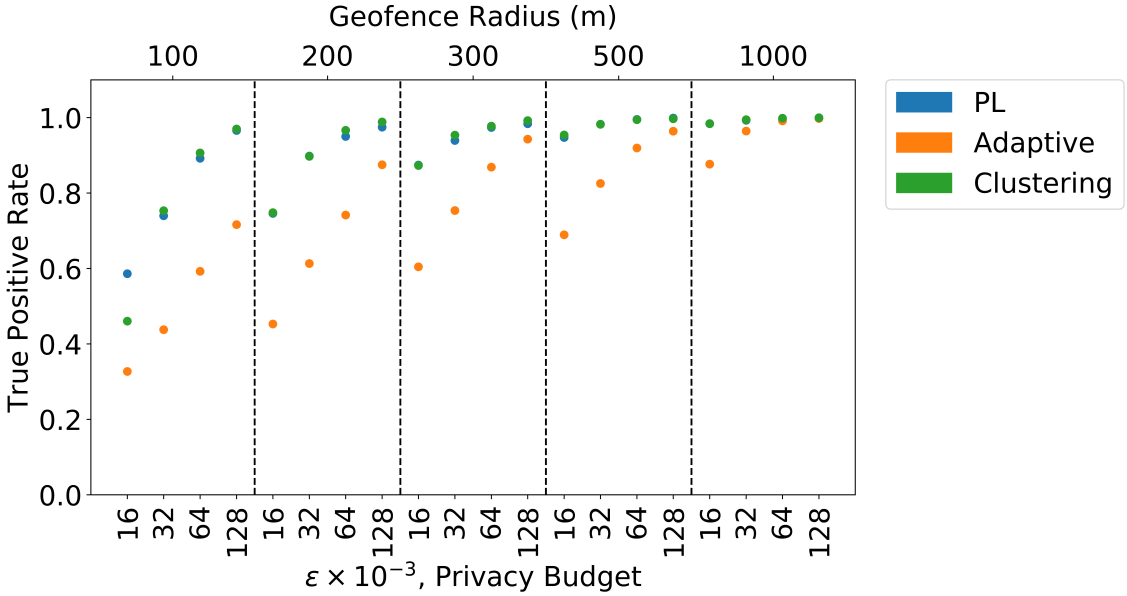


Figure 4.8: Comparison between the TPR of the PL, the adaptive geo-indistinguishability and the clustering geo-indistinguishability for the average of the Δ_t values and for different values of geofence radius and epsilon ϵ.

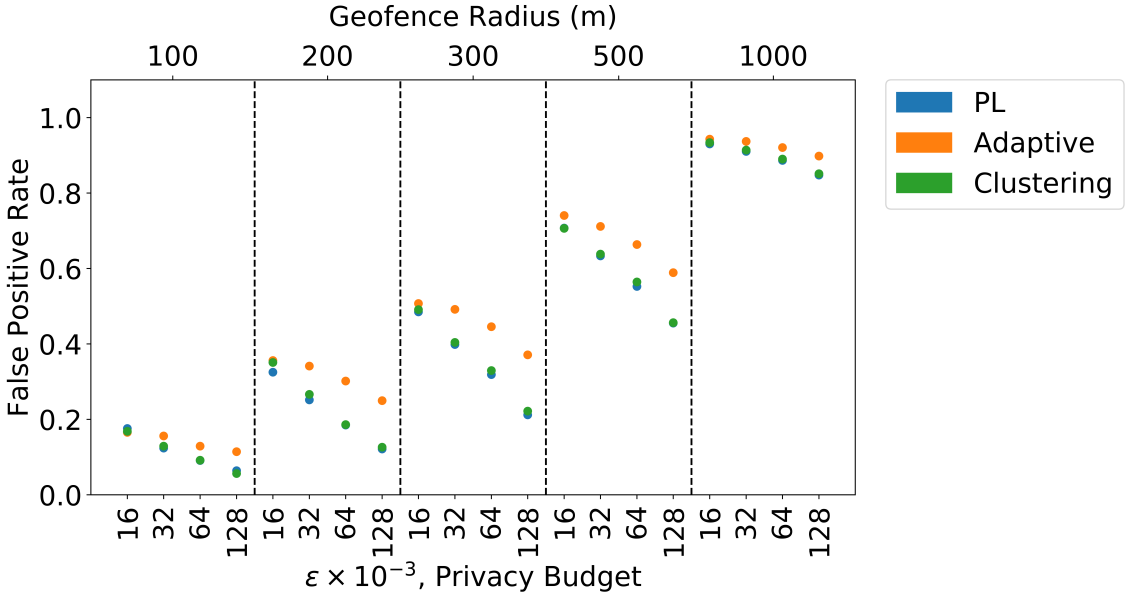


Figure 4.9: Comparison between the FPR of the PL, the adaptive geo-indistinguishability and the clustering geo-indistinguishability for the average of the Δ_t values and for different values of geofence radius and epsilon ϵ.

4.2.4 Trade-off Between Privacy and Utility Evaluation

According to the performed evaluation of both the privacy and the utility level of the mechanisms, we can conclude how the mechanisms lead with the trade-off between privacy

and utility. In comparison with the PL mechanism, the clustering geo-indistinguishability improves the privacy level for continuous reports of location data (i.e. lower values of Δ_t), with little to no penalty in terms of utility loss (measured by TPR), except for the case of the combined lowest epsilon and lowest geofence radius explained earlier. The comparison of our clustering scheme with adaptive geo-indistinguishability shows that the adaptive mechanism is able to achieve higher privacy levels (i.e. lower F_1 scores) for continuous scenarios (smaller Δ_t values), albeit at a severe cost in terms of utility, as shown in the practical geofence analysis. Therefore, we can conclude that the clustering geo-indistinguishability provides a favourable trade-off between privacy and utility for continuous reports.

Chapter 5

Conclusion

Location privacy is an emerging topic of research due to the pervasiveness of Location-Based Services (LBSs). Regardless of the benefits that these services offer to users, the shared data are not always and only used for the initial purpose. In order to protect the users, Location Privacy-Preserving Mechanisms (LPPMs) have been proposed. Our objective was to develop a mechanism that protects users not only against single reports but also over time, against continuous reports. Toward this goal, we developed a new mechanism that is suitable for continuous reports of location data and that improves the level of privacy for continuous reports, with limited or no loss in terms of utility.

To achieve our goal, we started by studying the state of the art of the existing techniques. Building from this knowledge, we evaluated how an obfuscation LPPM protects the privacy level of the users and what is the effect of the frequency of updates on location privacy. It was possible to assess the effect of the obfuscation level given by the geo-indistinguishability privacy parameter ϵ, being that a lower value of ϵ corresponds to a higher level of obfuscation. The obtained results allowed us to observe the impact of the frequency of updates in tracking attacks, even using an LPPM for sporadic scenarios or for continuous scenarios. In particular, we conclude that a lower frequency of updates degrades the effectiveness of the tracking attack and, consequently, improves the obtained privacy level.

The second part of the thesis was focused on the development and evaluation of a privacy-enhancing mechanism for location privacy. To develop the mechanism, we took into consideration the geo-temporal correlations, namely the distance between the reported locations and the frequency of updates. Thus, we created a clustering geo-indistinguishability mechanism that creates obfuscation clusters for closer locations, such that the mechanism returns the same obfuscated point for nearby locations. According to the performed analysis, our mechanism improves the privacy level in comparison with the Planar Laplace (PL) mechanism, with little to no loss in terms of utility. Moreover, although the adaptive geo-indistinguishability exhibits higher privacy levels, it does so at the cost of an undesirably high loss of utility, as shown by our analysis of a practical geofence application.

Finally, we can conclude that the objectives of this thesis were achieved. Besides the accomplishment of the tasks defined in the work plan, additional tasks were performed, such as the adaptation of an existing tracking attack according to the implemented LPPM and the evaluation of the utility of LPPMs through a real use-case based on geofencing. The main contributions of this thesis were the evaluation of the impact of the frequency of reports on location privacy, already reported in a submitted scientific article, and the development and evaluation of a new LPPM that protects the users in both the continuous and the sporadic scenarios while assuring relevant level of data utility.

5.1 Future Work

As future work, we would like to perform more experiments with other configurations of the implemented mechanisms, namely, more values of ϵ and different parameters for the adaptive geo-indistinguishability and for the clustering geo-indistinguishability. In this latter, we would like to study the effect of using the radius r_p, i.e. the radius of the circular region centred around the true location x where the obfuscated location z can appear with a certain probability p, instead of using the radius of obfuscation r. Moreover, we would like to compare with more LPPMs, such as the work that protects the users' locations with differential privacy under temporal correlations by using discretization [19]. Regarding the attacks, we would like to implement the Kalman filter as an attack to location privacy and compare its efficiency with the Map-Matching (MM) approach.

Moreover, we would like to develop a new mechanism that dynamically updates the value of ϵ based on the velocity of the user and the velocity of reporting. We started by exploring this idea and it seems a promissing approach to investigate. According to our idea, we would adapt the obfuscation of the locations based on the correlation between reports. For instance, since a higher velocity of the user corresponds to sparse locations and a higher velocity of reporting corresponds to closer locations, we could adapt the obfuscation level as a function of both the velocity of the user and the velocity of reporting. Moreover, in order to improve the privacy and utility of the mechanism, we could combine the new approach with our clustering approach. Thus, we could create obfuscation clusters for closer locations and update dynamically the value of ϵ for the remaining locations.

References

[1] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik. Your apps know where you were last night, and they're not keeping it secret. *The New York Times*, 2018. URL `https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html`. (consulted in January 2019).

[2] Paul Vines, Franziska Roesner, and Tadayoshi Kohno. Exploring adint: Using ad targeting for surveillance on a budget-or-how alice can buy ads to track bob. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society*, pages 153–164. ACM, 2017.

[3] The United Nations. Universal declaration of human rights, December 1948.

[4] Council of Europe. European convention on human rights, November 1950.

[5] European Union. Charter of fundamental rights of the european union, 2010.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L119:1–88, May 2016.

[7] A.F. Westin. *Privacy and Freedom*. Bodley Head, 1970. ISBN 9780370013251.

[8] Andrew J Blumberg and Peter Eckersley. On locational privacy, and how to avoid losing it forever. *Electronic frontier foundation*, 10(11), 2009.

[9] Iasonas Polakis, George Argyros, Theofilos Petsios, Suphannee Sivakorn, and Angelos D Keromytis. Where's wally?: Precise user discovery attacks in location proximity services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 817–828. ACM, 2015.

[10] Galini Tsoukaneri, George Theodorakopoulos, Hugh Leather, and Mahesh K Marina. On the inference of user paths from anonymized mobility data. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, pages 199–213. IEEE, 2016.

[11] John Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.

[12] Chaoming Song, Zehui Qu, Nicholas Blumm, and Albert-László Barabási. Limits of predictability in human mobility. *Science*, 327(5968):1018–1021, 2010.

[13] Yves-Alexandre De Montjoye, César A Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. *Nature Scientific reports*, 3:1376, 2013.

[14] Ricardo Mendes and João P. Vilela. Privacy-preserving data mining: Methods, metrics, and applications. *IEEE Access*, 5:10562–10582, June 2017.

[15] Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, and Yong Xiang. Location privacy and its applications: A systematic study. *IEEE Access*, 6:17606–17624, 2018.

[16] Reza Shokri, George Theodorakopoulos, and Carmela Troncoso. Privacy games along location traces: A game-theoretic framework for optimizing location privacy. *ACM Transactions on Privacy and Security (TOPS)*, 19(4):11, 2017.

[17] Reza Shokri, George Theodorakopoulos, George Danezis, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Quantifying location privacy: the case of sporadic location exposure. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 57–76. Springer, 2011.

[18] Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. Quantifying location privacy. In *2011 IEEE symposium on security and privacy*, pages 247–262. IEEE, 2011.

[19] Yonghui Xiao and Li Xiong. Protecting locations with differential privacy under temporal correlations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1298–1309. ACM, 2015.

[20] Hai Liu, Xinghua Li, Hui Li, Jianfeng Ma, and Xindi Ma. Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services. In *INFOCOM 2017-IEEE Conference on Computer Communications, IEEE*, pages 1–9. IEEE, 2017.

[21] Marius Wernke, Pavel Skvortsov, Frank Dürr, and Kurt Rothermel. A classification of location privacy attacks and approaches. *Personal and ubiquitous computing*, 18 (1):163–175, 2014.

[22] Miguel Andrés, Nicolás Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. In *20th ACM Conference on Computer and Communications Security*, pages 901–914. ACM, 2013.

[23] Konstantinos Chatzikokolakis, Ehab Elsalamouny, and Catuscia Palamidessi. Efficient utility improvement for location privacy. *Proceedings on Privacy Enhancing Technologies*, 2017(4):308–328, 2017.

[24] Simon Oya, Carmela Troncoso, and Fernando Pérez-González. A tabula rasa approach to sporadic location privacy. *arXiv preprint arXiv:1809.04415*, 2018.

[25] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh. An anonymous communication technique using dummies for location-based services. In *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*, pages 88–97. IEEE, 2005.

[26] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh. Protection of location privacy using dummies for location-based services. In *Data Engineering Workshops, 2005. 21st International Conference on*, pages 1248–1248. IEEE, 2005.

[27] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services*, pages 31–42. ACM, 2003.

[28] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Preserving privacy in gps traces via uncertainty-aware path cloaking. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 161–171. ACM, 2007.

[29] Gabriel Ghinita, Maria Luisa Damiani, Claudio Silvestri, and Elisa Bertino. Preventing velocity-based linkage attacks in location-aware applications. In *Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pages 246–255. ACM, 2009.

[30] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Marco Stronati. Geo-indistinguishability: A principled approach to location privacy. In *International Conference on Distributed Computing and Internet Technology*, pages 49–72. Springer, 2015.

[31] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Marco Stronati. A predictive differentially-private mechanism for mobility traces. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 21–41. Springer, 2014.

[32] Raed Al-Dhubhani and Jonathan M Cazalas. An adaptive geo-indistinguishability mechanism for continuous LBS queries. *Wireless Networks*, 24(8):3221–3239, 2018.

[33] John Krumm. Inference attacks on location tracks. In *International Conference on Pervasive Computing*, pages 127–143. Springer, 2007.

[34] Nilothpal Talukder and Sheikh Iqbal Ahamed. Preventing multi-query attack in location-based services. In *Proceedings of the third ACM conference on Wireless network security*, pages 25–36. ACM, 2010.

[35] Reza Shokri, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Protecting location privacy: optimal strategy against localization attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 617–627. ACM, 2012.

[36] Simon Oya, Carmela Troncoso, and Fernando Pérez-González. Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1959–1972. ACM, 2017.

[37] Mohammed A Quddus, Washington Y Ochieng, and Robert B Noland. Current map-matching algorithms for transport applications: State-of-the art and future research directions. *Transportation research part c: Emerging technologies*, 15(5):312–328, 2007.

[38] Mahdi Hashemi and Hassan A Karimi. A critical review of real-time map-matching algorithms: Current issues and future directions. *Computers, Environment and Urban Systems*, 48:153–165, 2014.

[39] Matej Kubicka, Arben Cela, Hugues Mounier, and Silviu-Iulian Niculescu. Comparative study and application-oriented classification of vehicular map-matching methods. *IEEE Intelligent Transportation Systems Magazine*, 10(2):150–166, 2018.

[40] Paul Newson and John Krumm. Hidden markov map matching through noise and sparseness. In *Proceedings of the 17th ACM SIGSPATIAL international conference on advances in geographic information systems*, pages 336–343. ACM, 2009.

[41] George R Jagadeesh and Thambipillai Srikanthan. Online map-matching of noisy and sparse location data with hidden markov and route choice models. *IEEE Transactions on Intelligent Transportation Systems*, 18(9):2423–2434, 2017.

[42] Isabel Wagner and David Eckhoff. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)*, 51(3):57, 2018.

[43] Pierangela Samarati and Latanya Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, technical report, SRI International, 1998.

[44] Pierangela Samarati and Latanya Sweeney. Generalizing data to provide anonymity when disclosing information. In *PODS*, volume 98, page 188. Citeseer, 1998.

[45] Traian Marius Truta and Bindu Vinay. Privacy protection: p-sensitive k-anonymity property. In *22nd International Conference on Data Engineering Workshops (ICDEW'06)*, page 94. IEEE, 2006.

[46] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam. ℓ-diversity: Privacy beyond k-anonymity. In *22nd International Conference on Data Engineering (ICDE'06)*, page 24. IEEE, 2006.

[47] Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, Tom H Luan, and Haibo Zhou. Silence is golden: Enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks. *IEEE Trans. Vehicular Technology*, 65(12):9942–9953, 2016.

[48] Cynthia Dwork. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pages 1–19. Springer, 2008.

[49] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing location privacy for vanet. Technical report, Washington Univ Seattle Dept of Electrical Engineering, 2005.

[50] Simon Oya, Carmela Troncoso, and Fernando Pérez-González. Is geo-indistinguishability what you are looking for? In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society*, pages 137–140. ACM, 2017.

[51] Avrim Blum, Katrina Ligett, and Aaron Roth. A learning theory approach to noninteractive database privacy. *Journal of the ACM (JACM)*, 60(2):12, 2013.

[52] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[53] Ricardo Mendes and João Vilela. On the effect of update frequency on geo-indistinguishability of mobility traces. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 271–276. ACM, 2018.

[54] Edsger W Dijkstra. A note on two problems in connexion with graphs. *Numerische mathematik*, 1(1):269–271, 1959.

[55] Michal Piorkowski, Natasa Sarafijanovic-Djukic, and Matthias Grossglauser. CRAWDAD dataset epfl/mobility (v. 2009-02-24). Downloaded from `https://crawdad.org/epfl/mobility/20090224`, February 2009. (consulted in January 2019).

[56] Lorenzo Bracciale, Marco Bonola, Pierpaolo Loreti, Giuseppe Bianchi, Raul Amici, and Antonello Rabuffi. CRAWDAD dataset roma/taxi (v. 2014-07-17). Downloaded from `https://crawdad.org/roma/taxi/20140717`, July 2014. (consulted in January 2019).

[57] Yu Zheng, Lizhu Zhang, Xing Xie, and Wei-Ying Ma. Mining interesting locations and travel sequences from gps trajectories. In *Proceedings of the 18th international conference on World wide web*, pages 791–800. ACM, 2009.

[58] Pablo Samuel Castro, Daqing Zhang, Chao Chen, Shijian Li, and Gang Pan. From taxi gps traces to social and community dynamics: A survey. *ACM Computing Surveys (CSUR)*, 46(2):17, 2013.

[59] Chong Yang Goh, Justin Dauwels, Nikola Mitrovic, Muhammad Tayyab Asif, Ali Oran, and Patrick Jaillet. Online map-matching based on hidden markov model for real-time traffic sensing applications. In *Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on*, pages 776–781. IEEE, 2012.

[60] Geoff Boeing. Osmnx: New methods for acquiring, constructing, analyzing, and visualizing complex street networks. *Computers, Environment and Urban Systems*, 65: 126–139, 2017.

[61] Aric Hagberg, Pieter Swart, and Daniel S Chult. Exploring network structure, dynamics, and function using networkx. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2008.

[62] Android Developers. Create and monitor geofences. URL `https://developer.android.com/training/location/geofencing.html`. (consulted in June 2019).

This page is intentionally left blank.

Appendices

This page is intentionally left blank.

Appendix A

Work Plan

This appendix describes the work plan for the first and for the second semester, which is presented in the first and in the second sections, respectively.

A.1 First Semester

According to the work plan proposed for this thesis, the first semester was focused in studying the state of the art related to location privacy, namely, privacy-enabling mechanisms for LBSs, methods to compromise location privacy and measures/metrics of privacy and utility. These topics are related to the privacy paradigm, which implies the definition of a protection mechanism, an attacker model and a measure/metric of privacy. The study of the state of the art and the analysis of the related works guaranteed the necessary knowledge for this thesis.

Besides the study of the state of the art, the goals for the first semester were the selection and the implementation of protection mechanisms and attacks, the evaluation of the privacy and utility of the mechanisms implemented and the writing of the intermediate report.

Furthermore, for the evaluation of the privacy and the utility of the implemented mechanisms, a real dataset was selected and pre-processed, and a road network was identified and incorporated as required by the implemented attacks.

Figure A.1 presents the tasks performed during the first semester through a Gantt chart.

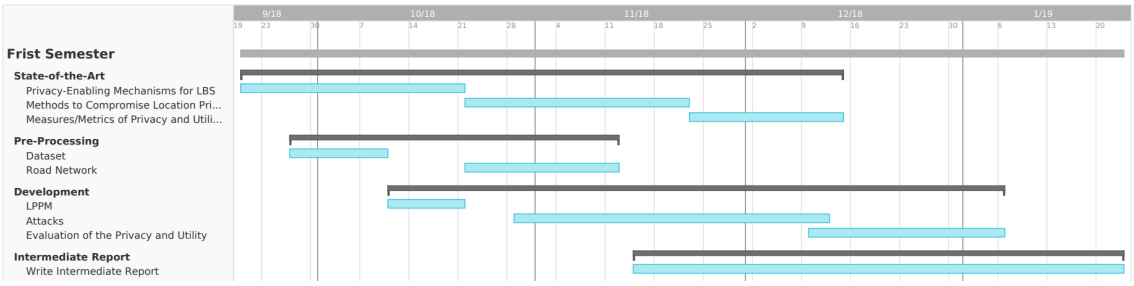


Figure A.1: Gantt chart for the first semester.

A.2 Second Semester

Aside from the continuation of the implementation and evaluation of different protection mechanisms and attacks started in the first semester, the work plan for the second semester consisted in three main tasks.

The first task was the evaluation of the impact of the frequency of updates in the privacy and utility of attacks and protection mechanisms. As shown in Chapter 3, in the first semester it was performed an evaluation of that impact for the implemented protection mechanism and attacks.

The second task consisted in the development of a privacy-enhancing mechanism for location privacy that is suitable to different frequency of updates and/or to the correlation between reports.

The third task consisted in the implementation and evaluation of the privacy-enhancing mechanism taking into consideration the utility and privacy levels achieved.

The last task was writing the final report and a scientific article where the contributions of this thesis were summarised.

Figure A.2 presents a Gantt chart with the tasks mentioned above and the planned scheduling made in the first semester.

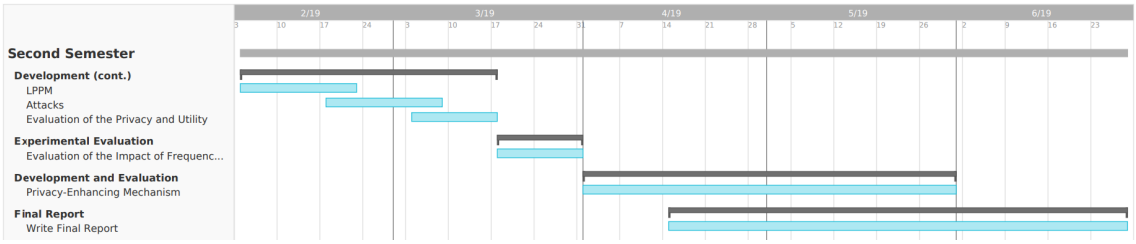


Figure A.2: Gantt chart for the second semester.

Figure A.3 shows the Gantt chart of the second semester with the revised scheduling. The main difference between the charts is the duration of the implementation and evaluation of the privacy-enhancing mechanism. In fact, the task took more time than the foreseen because we decided to evaluate the utility of our mechanism in a real use-case, as explained in Chapter 4.

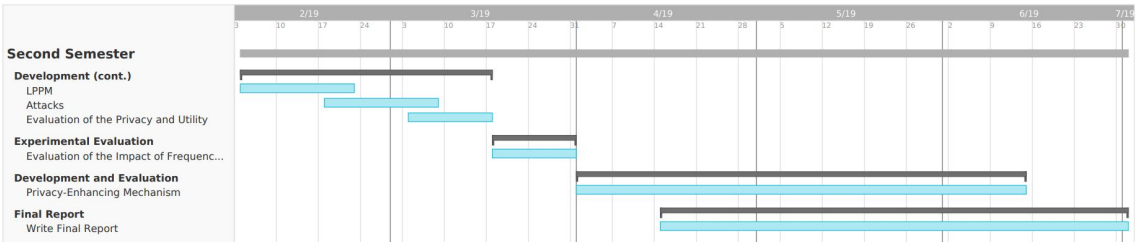


Figure A.3: Revised Gantt chart for the second semester.

Appendix B

Estimation of Map-Matching Parameters

This appendix details the estimation of the MM parameters λ_y and λ_z, following the proposal of the authors in [41]. The parameters are used to compute the transition probability in the MM technique. This probability depends on both the circuitousness of the path and the temporal implausibility, which in turn depend on the parameters λ_y and λ_z, respectively.

To estimate λ_y and λ_z, we measured the circuitousness (c.f. equation (3.6)) and the temporal implausibility (c.f. equation (3.7)) for a selected group of trajectories. In the original work, the authors observed that about 95% of the considered paths had the value of temporal implausibility equal to 0. However, since these paths are not relevant to estimate the parameters, the authors considered only the paths with non-zero temporal implausibility. In our work, we also observed a high number of paths with temporal implausibility equal to 0 and, consequently, we discarded them. From the remaining obtained values, we created the histograms for both the circuitousness and the temporal implausibility, as shown in Figure B.1 and Figure B.2. Then, we calculated the exponential distribution of each histogram, which is represented with an orange line. The value of λ_y and λ_z correspond to the rate parameter of these distributions, which can be estimated as the inverse of the average of all measured values. Regarding the selection of the trajectories, in the original work [41] the authors used the paths with duration between 1 and 5 minutes, resulting in 4828 trajectories with an average length of 2.6 km. In the same way, we used the trajectories with duration between 1 and 5 minutes that had at least 2 km of travelled distance, resulting in 6003 trajectories. The estimation of the parameters resulted in the following values: $\lambda_y \approx 0.07$ and $\lambda_z \approx 0.74$.

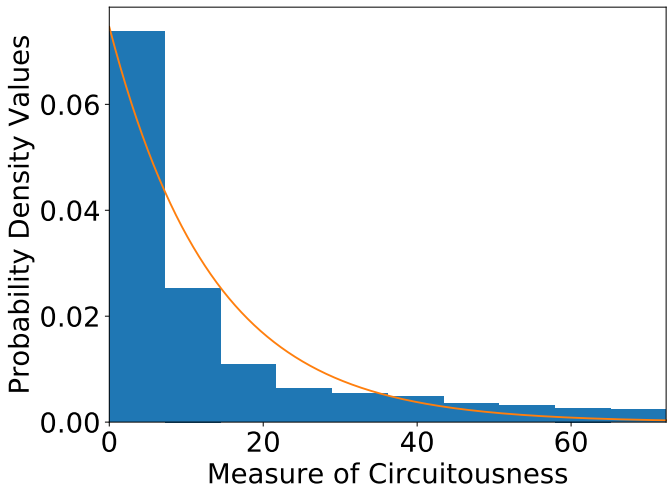


Figure B.1: Histogram of the circuitousness of the trajectories between 1 and 5 minutes that had at least 2 km of travelled distance, where the orange line represents the exponential distribution.

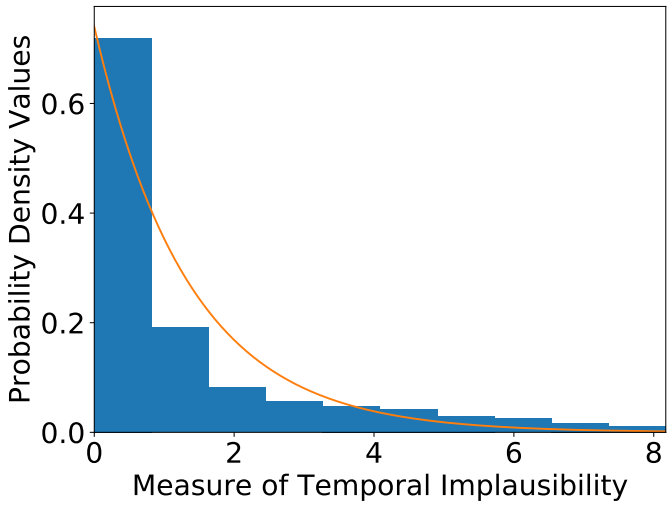


Figure B.2: Histogram of the temporal implausibility of the trajectories between 1 and 5 minutes that had at least 2 km of travelled distance, where the orange line represents the exponential distribution.