Quantifying Location Privacy In Location-based Services

by

Peiyuan Liu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2018

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Mobile devices (e.g., smart phones) are widely used in people's daily lives. When users rely on location-based services in mobile applications, plenty of location records are exposed to the service providers. This causes a severe location privacy threat. The location privacy problem for location-based services in mobile devices has drawn much attention. In 2011, Shokri et al. proposed a location privacy framework that consists of users' background knowledge, location privacy preserving mechanisms (LPPMs), inference attacks, and metrics. After that, many works designed their own location privacy frameworks based on this structure. One problem of the existing works is that most of them use cell-based location privacy frameworks to simplify the computation. This may result in performance results that are different from those of more realistic frameworks. Besides, while many existing works focus on designing new LPPMs, we do not know how different the location information an adversary can obtain is, when users use different LPPMs. Although some works propose new complementary privacy metrics (e.g., geo-indistinguishability, conditional entropy) to show their LPPMs are better, we have no idea how these metrics are related to the location information an adversary can obtain. In addition, previous works usually assume a strong or weak adversary who has complete background knowledge to construct a user's mobility profile, or who has no background knowledge about a user, respectively. What the attack results would be like when an adversary has different amounts of background knowledge, and can also take semantic background knowledge into account, is unknown.

To address these problems, we propose a more realistic location privacy framework, which considers location points instead of cells as inputs. Our framework contains both geographical background knowledge and semantic background knowledge, different LPPMs with or without the geo-indistinguishability property, different inference attacks, and both the average distance error and the success rate metrics. We design several experiments using a Twitter check-in dataset to quantify our location privacy framework from an adversary's point of view. Our experiments show that an adversary only needs to obtain 6% of background knowledge to infer around 50% of users' actual locations that he can infer when having full background knowledge; the prior probability distribution of an LPPM has much less impact than the background knowledge; an LPPM with the geo-indistinguishability property may not have better performance against different attacks than LPPMs without this property; the semantic information is not as useful as previous work shows. We believe our findings will help users and researchers have a better understanding of our location privacy framework, and also help them choose the appropriate techniques in different cases.

Acknowledgements

I would like to thank my supervisor Urs Hengartner, for his advising and considerable help with this research. Also, I would like to thank my thesis committee members Ian Goldberg and Florian Kerschbaum, for their valuable feedback on this thesis.

This work benefitted from the use of the CrySP RIPPLE Facility at the University of Waterloo.

Dedication

To my parents, for the love and support, and Zuoming, whose companionship helped me get through the days.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

Mobile devices (e.g., smart phones) are widely used in people's daily lives. These devices are usually equipped with high-precision localization capabilities, such as GPS receivers. Many mobile applications provide convenience to the device owners by requesting users' current locations to provide their services. While many users rely on the location-based services (LBSs) in mobile applications, plenty of location records are exposed to the service providers. This causes a severe location privacy threat. Considering that an external attacker may find a way to steal this information, and the service providers themselves can be malicious, such an adversary may be able to approximate a user's location or even locate a user' precise position in real time.

The location privacy problem for location-based services in mobile devices has drawn much attention [WSDR14]. To protect users' location privacy, a useful strategy is to add noise to users' actual locations when people expose their locations to location-based services. By limiting the scale of the noise, people can still keep some utility of an LBS when protecting their location privacy. The mechanisms to generate such noise are called location privacy preserving mechanisms (LPPMs). To evaluate the protection mechanisms, several inference attacks and privacy metrics have been proposed [STD$^+$11,Sho15,ABCP13, OTPG17a]. Different designs of these components compose various location privacy frameworks.

While many location privacy works have been presented to discuss different LPPMs, attacks, metrics, and entire frameworks, some problems emerge. Most of the existing works only focus on coarse-grained cell-based location privacy frameworks. They divide the location area into large cells, in order to simplify the computation. These frameworks are so simplified that they may lead to very good experimental results, which may not be the same when using a more realistic framework. For example, Agir et al. [AHHH16] use a simplified framework to prove that semantic information (e.g., hospital, gym, bar) has a large impact on the attack results, because using a cell as a unit that contains many location points loses much information of these location points. If we use each location point as a unit, the semantic information may not be as informative as people think it is. Besides, most previous works consider background knowledge in their frameworks, but they either assume the worst case that the adversary knows users' entire mobility profile, or do not indicate how much knowledge the adversary has. We do not know how different the performance of the LPPMs, attacks or metrics will be when the adversary has different amounts of background knowledge. Also, the prior probability distribution of an LPPM and the background knowledge are two major factors of the attack performance. While many works are engaged in improving the performance of LPPMs, it is unclear how much impact the LPPM has against different attacks, and what the limitations of improving the LPPMs are. In addition, the geo-indistinguishability metric [ABCP13] has become popular recently, but a study on the impact of geo-indistinguishability is needed to tell how much people should rely on it when designing LPPMs. The details of the problems above are analyzed in Chapter 2.

1.2 Goals

In this thesis, we focus on quantifying location privacy for location-based services from an adversary's point of view. To be specific, we aim at studying the impacts of different components of a location privacy framework on the performance of different attacks. We present a location privacy framework. Using this framework, our goal is running experiments to answer the following questions:

- Does an adversary need a large amount of background knowledge to infer users' locations?
- How much impact does the prior probability distribution of an LPPM have on inference attacks?
- Is an LPPM with the geo-indistinguishability property always better than an LPPM without this property?

- Does semantic information have as large an impact on inference attacks as people expect?

1.3 Contributions

Instead of the cell-based framework, we present a more realistic location privacy framework that considers location points in a check-in dataset. The location privacy framework is composed of different types and amounts of background knowledge, location privacy preserving mechanisms, inference attacks, and metrics. Using this framework, we quantify location privacy for location-based services from the adversary's point of view. That is, we run several experiments to evaluate how much impact each component of the framework has on the adversary's attack results. The main contribution is answering the four questions in Section 1.2, and drawing the following conclusions:

- We present a way to quantify the different amounts of background knowledge about users. Our experiments show that the success rate of the adversary rockets as soon as the adversary has some background knowledge about a user. An adversary only needs to obtain 6% of background knowledge to infer around 50% of users' actual locations that he can infer when having full background knowledge. This is arguably different from people's intuition.

- The prior probability distribution of an LPPM and the amount of background knowledge are two major factors that affect the results of inference attacks. Our experiments show that, no matter how much background knowledge the adversary has, the adversary can achieve overall 80% of the success rate that he can achieve when also using the prior probability distribution of the LPPM in the attack. The quality loss (i.e., the average distance between the actual locations and the fake locations generated by the LPPM) varies from 0.1 km to 1 km.

- We compare different LPPMs with and without the geo-indistinguishability property. We already know that compared with undesirable LPPMs (e.g., the coin mechanism [OTPG17a]), a good LPPM with the geo-indistinguishability property is better [ABCP13, OTPG17a]. Our experimental results show that compared with other good LPPMs, however, an LPPM with the geo-indistinguishability property does not have a better performance against different attacks.

- We design two Bayesian inference attacks with extra semantic knowledge. Compared to the original Bayesian inference attack with only geographical background knowledge, the experimental results show that the semantic background knowledge is not helpful in most of the cases, but semantic background knowledge can help the attacker infer a user's locations when the user goes to a new area.

This thesis is organized as follows: Chapter 2 introduces the background and related work. Chapter 3 presents each part of our framework in detail. Chapter 4 describes the implementation, results, and observations of our experiments. Possible future work is discussed in Chapter 5. Chapter 6 shows the conclusions.

Chapter 2

Background And Related Work

Researchers have been interested in location privacy for many years. Many techniques have been proposed to protect location privacy.

One of the techniques is anonymization. The idea is hiding user identities so that an adversary is unable to link disclosed location data to the corresponding user. For example, we can use pseudonyms to replace the user identities. However, Bettini et al. [BWJ05] show that consecutively disclosing multiple locations of a user can become a quasi-identifier to identify the user. K-anonymity [Swe02] is another widely used technique in the data privacy field that can be used to protect location privacy. Gruteser and Grunwald [GG03] first applied k-anonymity to location privacy. Their idea is building a geographical cloaking area which at least another $k-1$ users are in, in order to make each user indistinguishable from each other. Considering that k-anonymity is vulnerable to an adversary with semantic knowledge of users' data, Xiao et al. [XXM08] and Xue et al. [XKP09] use the idea of l-diversity [MGKV06] to propose semantic-aware protection mechanisms for location privacy. A typical drawback of such k-anonymity works [GG03,LLV07,GL08,XXM08,XKP09,XC09] is that they rely on a trusted third-party to be the anonymizer. Overall, anonymization in location privacy has been extensively studied, but later works show anonymization is actually quite ineffective [GH05, GP09, ZB11]. Linking a user to his anonymized location records is easy, especially when the adversary knows the user's historical location data.

Obfuscation is the most commonly used technique to protect location privacy now. The idea of location obfuscation was first proposed by Duckham and Kulik [DK05]. They formalized the notions of inaccuracy and imprecision. To be specific, inaccuracy means providing a location measurement different from the real one; imprecision means reporting a larger area instead of the real location. Various obfuscation mechanisms have been proposed in recent years. We will discuss them in detail in the following sections.

Besides anonymization and obfuscation, some cryptographic protocols [DD11, CSPE12, HRDP14] have been proposed to protect privacy in location sharing. Such protocols require technical modifications of the location-based services. Another two cryptographic protocols [ZGH07, MGBF14] also provide features for preserving location privacy, but they require careful analyses and extensions to incorporate the features in the location-based services. Overall, these protocols are designed to protect users' location privacy in specific applications. It is not straightforward to adjust them to fit in the general cases where people tend to expose their current locations to the location-based services in real time.

In this thesis, we will focus on location obfuscation. Shokri et al. [STLBH11] propose a location privacy framework that contains four components: background knowledge, obfuscation mechanisms, inference attacks, and metrics. Although later works use different mechanisms, attacks or metrics, the structure of Shokri's framework is considered as a standard, remaining unchanged. Therefore, we will also follow this structure, and introduce the related work of each component in the following sections.

2.1 Background Knowledge of Users' Mobility Profiles

The knowledge of users' mobility profiles is the prior information about users' previous location data that an adversary obtains from many approaches, such as social networks, location data released by service providers, location data leakage, and personal knowledge.

2.1.1 Personalized And Aggregated Background Knowledge

Usually what an adversary considers as background knowledge is the latitude, longitude, and time of each user's previous location records, called geographical background knowledge. When an adversary constructs the background knowledge using a single user's location data, we call it personalized knowledge. The general knowledge of a crowd consisting of the location data for all users is known as aggregated knowledge. In the sporadic case when a user occasionally reports his locations to the location-based service providers, the knowledge of the user's mobility pattern is represented as their geographical distribution over the points of interest [STD+11]. That is, the probability distribution of the user's location data. In the continuous case when a user frequently reports his locations, the knowledge is the user's probability distribution of transitions between the points of interest [STLBH11]. The background knowledge is represented as the conditional probability distribution of the user's location data, given his previous locations. The detail will be described in Chapter 3.

Personalized knowledge has been used in many papers [AHHH16,OTPG17a,STLBH11, STD$^+$11,STT$^+$12,YLP17]. They assume an adversary has some prior knowledge of a user, and uses the knowledge in a Bayesian inference attack to infer the user's real location. Although in their experiments they evaluate their work with the background knowledge, none of them quantify the scale of the knowledge. The "some prior knowledge" vaguely described in the previous work could be only a little amount of knowledge that barely affects the attack results, or a large amount of knowledge that well reflects the user's mobility pattern and significantly improves the attack results. To give people a clearer understanding of how much impact the background knowledge has on the attack results, we will perform several experiments to quantify the background knowledge in Chapter 4.

Aggregated knowledge also affects users' location privacy, especially when an adversary is unable to obtain a single user's location data to construct personalized knowledge. Pyrgelis et al. [PTDC17] show that the aggregated knowledge improves the adversary's knowledge about users' mobility patterns and helps the adversary to localize users.

2.1.2 Semantic Background Knowledge

Semantic background knowledge is the semantic information of a location, such as "restaurant", "hotel", "gym", etc. When using location-based services, mobile users often not only share their geographical locations but also share the semantic information of their current locations. Besides, the semantic information can also be inferred from the geographical information of a location (e.g., if the location is a hospital, park, or school).

Agir et al. [AHHH16] investigate the impact of location semantics on location privacy by comparing the attack results of an adversary with only geographical background knowledge and an adversary with both geographical and semantic background knowledge. Their work is the first to formalize the problem, showing that users' semantic location privacy is a serious problem, and semantic information helps the inference of users' geographical locations. However, the result that semantic information has a large impact on location privacy can be misleading. First, this paper only considers the cloaking mechanism, which is weaker than some other obfuscation mechanisms (e.g., the planar Laplace mechanism) against inference attacks in terms of the average distance error metric [ABCP13]. Only considering the cloaking mechanism could result in better attack performance. Second, the cell-based framework loses part of the geographical information, because the user does not expose his specific location but an area (called a "cell") that covers his location. This causes the semantic information to become more informative than it is in reality. If we consider the precise locations of users and stronger inference attacks (e.g., attacks proposed by Shokri et al. [STLBH11, STD$^+$11, STT$^+$12]), the semantics can be less informative and thus have less impact on users' location privacy, as we will show in Chapter 4.

Some other works also consider semantics in location privacy. Damiani et al. propose a framework called PROBE [DBS$^+$10] to hide locations that have sensitive semantic information (e.g., hospital). PROBE allows users to specify the sensitivity level of each location type (e.g., restaurant, hospital, school), and develops a cloaking protection mechanism that guarantees the cloaking areas are under a certain sensitivity level. To some extent, PROBE is useful to protect user's location privacy when locations have sensitive semantic information, but it has many weaknesses. First, the cloaking region can be very large when this region contains many sensitive locations, which causes large utility loss. Second, PROBE can unintentionally indicate to an adversary what a user wants to protect, since a large cloaking region must contain very sensitive locations while a small cloaking region only contains less sensitive locations. Oya et al. [OTPG17a] also consider semantic information in their paper. However, they only evaluate the semantic location privacy in terms of the semantic privacy metric in Agir et al. [AHHH16], that is, how an adversary can infer the semantic information of each location when a user hides part of the semantic information. Their work does not use extra semantic information to infer users' geographical location privacy.

Although many existing works take semantic knowledge into account, they either only use semantic information to evaluate semantic location privacy, or use the cell-based framework, which can exaggerate the impact of semantic information. Therefore, we will introduce a practical location privacy framework, and show that semantic information does not have much impact on the attack results in Chapter 3 and Chapter 4.

2.2 Privacy Protection Mechanisms

Location privacy protection mechanisms (LPPMs) are designed to protect users' location privacy against inference attacks. An obfuscation mechanism is a function that maps a actual location to a random variable that represents one or several obfuscated locations. Obfuscation mechanisms covers various methods that reduce the accuracy/precision of users' actual locations: perturbation, adding dummy locations, reducing precision, and location hiding. [STLBH11]

2.2.1 Location Perturbation

A location perturbation mechanism is a function that adds noise to an input location. Some perturbation mechanisms are for discrete cases and others are for continuous cases according to whether the input locations are cell-based or not, and whether the output locations are discrete or continuous.

In the discrete case, the location area is divided into cells. An LPPM takes a cell as an input, and outputs another cell as the obfuscated location. For example, Shokri et al. [STT+12] propose an optimal strategy for location perturbation. It divides a $15.32\,\text{km}\times 7.58\,\text{km}$ area into 300 cells, each of which is $0.387\,\text{km}^2$. One weakness of the solution in the discrete case is that the algorithm has to traverse all the possible output locations. Due to computational limitations, people have to divide the map into large cells or only consider a small-sized map [AHHH16] in the evaluation. Also, several works propose new mechanisms that combine the Bayesian and the geo-indistinguishability approaches to have a good performance against the Bayesian adversary [Sho15, CPS15]. Yu et al. [YLP17] design an LPPM called PIVE that can improve the worst-case performance against inference attacks.

Most of the existing works only focus on the simplified cell-based frameworks, but in the real world, the locations are continuous. Recently Oya et al. [OTPG17a] study the performance of the LPPMs in the continuous case. "Continuous" means an LPPM considers each place (e.g., a restaurant, a building, a hotel) as an input location instead of considering a cell as a location, and outputs a continuous obfuscated location on the map (i.e., the latitude value and longitude value are continuous numbers). The obfuscated location can be any point in the given area. Uniform circular noise, bi-dimensional Gaussian noise, planar Laplace noise are the basic mechanisms [OTPG17a]. To study location privacy from a practical point of view, we only focus on the continuous case in this thesis.

2.2.2 Other Obfuscation Mechanisms

Besides location perturbation, there are also some other kinds of obfuscation mechanisms.

Adding dummy locations, also known as query obfuscation [Kru09, PS11, SGI09] is a mechanism to generate dummy locations. It does not hide the actual locations. Instead, for each query, this mechanism outputs both the actual location and several dummy locations to the service providers, so the adversary does not know which one is the real location. Unlike other protection mechanisms the output locations of which are different from the actual locations, this mechanism does not cause errors between the output locations and the actual locations. However, it causes some bandwidth problems.[1] If a user relies on this mechanism to protect his location privacy, the mechanism has to generate plenty of dummy locations and send them to the servers at the same time.

The precision reducing mechanism reduces the precision of a location by dropping the low-order bits of the location identifier [STLBH11]. The output is deterministic. The location hiding mechanism does not transmit the users location to the service provider with a certain probability [STLBH11]. Since both of them are cell-based we do not consider them in our analyses.

2.3 Evaluating Location Privacy

2.3.1 Inference Attacks

Inference attacks aim at inferring useful information from users' locations. Shokri et al. [STLBH11, STD$^+$11] propose a localization attack based on Bayesian inference. This Bayesian inference attack has been regarded as a standard, being widely used to evaluate the location privacy frameworks. As mentioned in Section 2.2.1, when talking about LPPMs, researchers consider the continuous case and the discrete case according to whether the output location is continuous or discrete [OTPG17a]. Similarly, researchers also need to consider two different cases of the inference attacks, according to whether the observed trace is continuous or sporadic [STLBH11, STD$^+$11].

In the continuous (not sporadic) case, the tracking attack targets the reconstruction of complete or partial actual traces (i.e., sequences of locations). Shokri et al. [STLBH11] propose two tracking attacks that make use of the knowledge of the transitions between locations. Agir et al. [AHHH16] also propose two attacks based on general Bayesian networks with or without extra semantic information. Different from the tracking attacks proposed by Shokri et al. [STLBH11], these two attacks only use the geographical and semantic background knowledge to infer users' location information, ignoring the prior probability distribution of LPPMs. In the sporadic case, the localization attack is defined to target a single location at a given time instant. The background knowledge an adversary uses is the probability distribution of different locations at each time period. The localization attack based on Bayesian inference [STLBH11, STD$^+$11] is widely used in location privacy research [YLP17, OTPG17a].

[1] In the continuous case (see Section 2.3.1), another hard problem is the generation of realistically looking dummy location traces. However, this thesis focuses on the sporadic case.

A disadvantage of the continuous (not sporadic) case is that it requires a large amount of location data to construct each user's transition matrix between locations. However, the available location datasets are limited. Agir et al. [AHHH16] use the cell-based framework to avoid this problem. In our work, we use the same dataset as Agir et al. [AHHH16], because this dataset is the only one we found that has semantic tags for each location record. Since we want to consider a more practical location privacy framework instead of the cell-based framework, we will only focus on the sporadic case in this thesis.

2.3.2 Privacy Metrics

Metrics are used to evaluate the performance of protection mechanisms and attacks.

The average error metric is a standard privacy metric with an arbitrary distance function. Many works consider this function as the Euclidean distance function, and use it to evaluate the average distance error between the adversary's inferred locations and users' actual locations [STT+12, STLBH11, STD+11, PTDC17, OTPG17a, YLP17]. If we consider this arbitrary function as 0 and 1, where 1 means the adversary successfully infers the actual location, and 0 means the adversary infers the wrong location, then the average error will become the success rate metric [YLP17]. The average distance error and the success rate are two privacy metrics that directly show what and how much information an adversary can obtain.

Geo-indistinguishability [ABCP13], which provides privacy guarantees independent of the adversary's prior, is another formalized privacy notion for LBS applications. It is based on a generalization of differential privacy [CABP13, Dwo06], used by many works [FS14, Sho15, KFS15, MC14, YLP17, OTPG17a]. One follow-up work [BCP14] uses an expensive linear programming algorithm to achieve optimal geo-indindistinguishability in terms of utility. Another work [CEP17] uses remapping methods to increase the utility of geo-indindistinguishable mechanisms. Geo-indistinguishability limits the information leakage through observation, but it does not consider the prior knowledge an adversary may have. Also, the privacy level defined by geo-indistinguishability does not directly reflect what is learned about users' location information. A recent work [OTPG17b] provides a numerical interpretation of this privacy guarantee, and points out that the geo-indistinguishable mechanisms have poorer performance than other noise generation mechanisms in terms of the average error metric.

Conditional entropy is a complementary metric that is used to avoid choosing undesirable mechanisms (e.g., the coin mechanism [OTPG17a]). It measures the adversary's uncertainty about users' actual locations. Similar to geo-indistinguishability, conditional entropy also does not explicitly reflect what is learned from an adversary's point of view.

2.4 Existing Evaluation Work

While plenty of new location privacy techniques have been proposed, only a few works focus on evaluating location privacy. The evaluating work is important, because it can point out the different behaviours of different location privacy works, helping people to choose which one to use in different situations and design new techniques. Shokri et al. [STLBH11, STD$^+$11] first proposed a standard location privacy framework to quantify location privacy. They provide a general idea about how to evaluate the privacy loss of the LPPMs, but they do not go into detail to compare different types and amounts of background knowledge, different LPPMs, different attacks and different metrics. Andres et al. [ABCP13] compare the planar Laplace mechanism with the cloaking mechanism, showing that the planar Laplace mechanism with the geo-indistinguishability property is better than the cloaking mechanism. However, the cloaking mechanism is not a mechanism that generates noise like the planar Laplace mechanism does. The question remains whether the planar Laplace mechanism with the geo-indistinguishability property is better than other noise generating mechanisms. Agir et al. [AHHH16] quantify the semantic location privacy, and show that the semantic background knowledge can significantly improve the inference attack performance. Yu et al. [YLP17] compare their LPPM called PIVE with the exponential mechanism and the optimal geo-indistinguishable mechanism, showing that their mechanism PIVE has better behaviours in the worst cases. One common drawback of the evaluation work above is that they are all based on the cell-based location privacy frameworks. Pyrgelis et al. [PTDC17] show that aggregated background knowledge helps the adversary to localize users. However, they use the cell-based framework as well for the epfl/mobility dataset [PSDG09]. For the other dataset being used in their work, although they do not consider a cell-based framework, this public transport in London dataset only contains the location records at different stations. Therefore, this work does not study people's daily movements, such as a person going to a restaurant, to a office, or home.

Oya et al. [OTPG17a] propose the coin mechanism and a mechanism with large conditional entropy to show that an LPPM can have good behaviour in terms of one metric while having bad behaviour in terms of another metric. In another work, Oya et al. [OTPG17b] redefine geo-indistinguishability as the minimal error of an adversary when he tries to distinguish between two possible real locations. This work shows that the planar Laplace mechanism with the geo-indistinguishability property needs to sacrifice more utility to guarantee the same privacy error as other mechanisms do. These existing works make several comparisons between different LPPMs and different metrics from the users' point of view, but it is important to let people realize what explicit information an adversary can obtain if a user chooses to use one LPPM instead of others in each situation. Therefore, our work focuses on evaluating the location privacy framework from an adversary's point of view.

2.5 Summary

Location privacy has been studied for years. Various protection mechanisms, metrics, and frameworks have been proposed and evaluated. However, most of them study location privacy from users' point of view, ignoring how an adversary can try his best to infer location information he wants to know, As a result, people are confused about which protection mechanisms/inference attacks to choose to protect/attack users' location privacy. To address the problem, we quantify sporadic user-centric location privacy for location-based services from the adversary's point of view.

In the following chapters, we will show how much information an adversary can obtain in terms of explicit privacy metrics, such as the average distance error metric and the success rate metric. We will quantify the impacts of different types and amounts of background knowledge (including semantic background knowledge), the prior probability distribution of an LPPM, different LPPMs with or without the geo-indistinguishability property, and different attacks.

Chapter 3

Quantifying Location Privacy Under Different Settings

While various attacks and defences have been proposed, there is a lack of analyses to help people to decide which attack and which defence to use in a certain situation. To address this problem, we design several experiments to show how different background knowledge, attacks, and LPPMs affect an adversary's attack results in terms of different metrics. In this chapter, we introduce the location privacy framework we use in our experiments, including Bayesian inference attacks with semantic information and analyses of different privacy metrics.

3.1 Overview of Location Privacy Framework

We first illustrate the location privacy problem under our location privacy framework based on Shokri et al.'s work [STLBH11]. We consider a set of users that occasionally send queries with their current locations to location-based services, and an adversary who is curious about users' current locations. To prevent the potential adversary from knowing the real locations while still obtaining services, users can perturb their locations using a location privacy-preserving mechanism (LPPM) before exposing the locations to location-based service providers. When observing some obfuscated locations, the adversary, who knows the LPPM operation and has some knowledge about users' mobility patterns, tries to infer users' real locations.

Considering a set of users U in a set of time periods T, we model all the possible real locations that may be queried by users as a discrete set of points of interest (PoIs) denoted

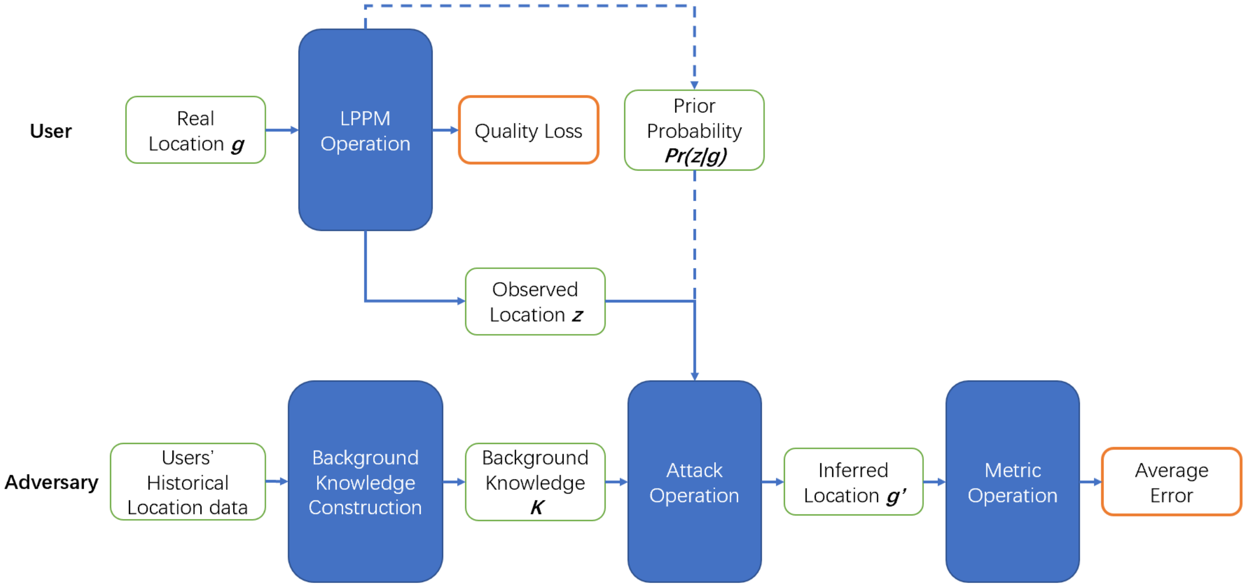

Figure 3.1: Location Privacy Framework

as G. The locations are discrete because we consider the scenario where users expose their locations like check-in data. We care about if a user is in this restaurant or that hotel instead of the precise coordinate of the user in a venue. The set of possible observed locations generated by LPPMs is denoted as $Z \in \mathbb{R}^2$. Note that fake location $z \in Z$ is not discrete, because in practice LPPMs can generate fake locations anywhere on the map. The protection mechanism is modeled as the conditional probability distribution $Pr(z|g)$, showing the probability of reporting an observed location $z \in Z$ given a real location $g \in G$. Note that for each g, z, we consider they are generated in a time period $t \in T$. Considering an adversary Adv with background knowledge K, we model the inference attack as a posterior probability distribution $Pr(g'|z)$, showing the probability of $g' \in G$ being the real location g given an observed location $z \in Z$. The performance of the protection mechanisms and the inference attacks are evaluated by quality loss metrics and privacy metrics. The entire defence and attack process is shown in Figure 3.1. The dotted line means the attacker can choose to use or not use the prior probability distribution $Pr(z|g)$ in the inference attacks.

Although our framework uses the same structure as the framework in Shokri et al. [STLBH11] does, the implementation of each component is quite different. For example, their framework is cell-based, but our framework considers each location point as the actual location, and our obfuscated locations are continuous (not discrete) on the map. The way to construct the background knowledge, the LPPMs, the attacks, and the metrics we use are all different from their framework. In the following sections, we will introduce each component in detail.

3.2 Adversary's Background Knowledge

An adversary's background knowledge K is built based on users' historical location data from many sources, such as social networks, location data released by service providers, location data leakage, and personal knowledge. Specifically, K_G is a $|G| \times |T|$ matrix representing the geographical background knowledge. Each element $K_G(g,t)$ represents the probability of a user visiting a PoI g in a time period t.

3.2.1 User's Information

A user's background knowledge is available to the adversary and originates from historical data belonging to this user. Usually, when talking about background knowledge, people refer to the geographical background knowledge. We consider the $|G| \times |T|$ ground truth matrix L_G^u of user u where $L_G^u(g,t)$ represents the number of times that user u visits a PoI g in a time period t. As known to the adversary, we build user's background knowledge as:

$$\forall g \in G, t \in T, K_G^u(g,t) = \frac{L_G^u(g,t)}{\sum_{j \in G} L_G^u(j,t)}$$

We denote a user's geographical mobility profile as $\pi_u(g,t)$, which is the probability of the user u being at the location g at the time period t. We have $\pi_u(g) = \sum_{t \in T} \pi_u(g,t)$. The data being used to construct the background knowledge can be limited, so an adversary may not know a user's complete mobility profile. If $\forall g \in G$ and $t \in T, K_G^u(g,t) = \pi_u(g,t)$, i.e., the adversary knows this user's complete mobility profile, we say the adversary has complete background knowledge of user u. Ideally, if an adversary has complete background knowledge about a user, inferring the user's current location can be relatively easy, but in real life, the adversary may only be able to obtain a little background information from a single user. In Chapter 4, we will show how different amounts of background knowledge will affect the attack results.

3.2.2 Geographical and Semantic Information

In general, what people consider as background knowledge is how users' geographical locations move over time, which are represented using longitudes and latitudes, or location IDs in our discrete case. However, a user's historical location records may not include the user's current location, thus geographical background knowledge cannot help the adversary to infer the user's location. In this case, the historical semantic information may be useful.

Semantic background knowledge considers the semantic tags of the PoIs that users' visit, such as "restaurant", "residence", "hospital". By constructing semantic background knowledge, an adversary can know users' location preferences that are not restricted to any specific PoI in different time periods. This can help an adversary to infer users' current locations when the geographical background knowledge is limited. For example, if a user usually goes to restaurants during this time period, and now this user is in an area where he has never been before, then the user may be in a new restaurant in this new area now. The set of possible semantic tags is S. The $|S| \times |T|$ ground truth matrix of user u is L_S^u where $L_S^u(s,t)$ represents the number of times that user u visits PoIs with the semantic tag s in a time period t. As known to the attacker, then the geographical background knowledge K_G and semantic background knowledge K_S are:

$$K_G^u(g,t) = \frac{L_G^u(g,t)}{\sum_{j \in G} L_G^u(j,t)} \text{ user's geographical background knowledge}$$

$$K_S^u(s,t) = \frac{L_S^u(s,t)}{\sum_{j \in S} L_S^u(j,t)} \text{ user's semantic background knowledge}$$

In this thesis, we will leave the superscript u of K^u away when it is clear from the context.

Semantic Tag Hierarchy

The problem of how to classify the semantic information of different locations is inevitable when considering semantic background knowledge in the inference attacks. It is hard to know what is the best classification of the semantic tags. In our framework, we choose the semantic tag categories in Foursquare [Fou18]. These categories compose a semantic tag hierarchy. For example, the semantic tags of a Szechuan restaurant can be "food"-"Asian restaurant"-"Chinese restaurant"-"Szechuan restaurant"; the semantic tags of a yoga studio can be "outdoor & recreation"-"athletics & sports"-"gym / fitness center"-"yoga studio".

3.2.3 Time Partition

Users usually have different behaviours in different time periods. For example, a user may go to his office in the morning, go to restaurants in the evening, and go home at night. Therefore, if this user has a high probability of being at restaurants during the day, this high probability needs to be constrained in the time period "evening", because the user seldom goes to restaurants in other time periods. In this thesis, we test several different time partitions, such as partitioning a day into 24 hours, considering a day as one time period, and partitioning a day into morning, afternoon and night. Then we choose the time partition that generates the best attack results. That is, we partition the time (e.g., a day) into five time periods (morning, lunchtime, afternoon, evening, and night), when building the background knowledge. Note that this may not the best time partition among all possible time partitions, but the best among all that we tested. The results presented in Chapter 4 are aggregated across this time partition. Besides partitioning the time in a day, we can also partition a week into work days and weekend, partition a year into four seasons, or partition a year into normal days and holidays. We leave testing other different time partitions as future work.

3.3 Location Privacy-Preserving Mechanisms

In this section, we introduce the location obfuscation mechanisms that we use in our framework.

A location obfuscation mechanism is defined as a prior probability distribution function $f(z|g)$ (or $Pr(z|g)$), where $z \in Z$ is an obfuscated location, and $g \in G$ is a user's actual location. The coordinate of g is denoted as (x, y), the coordinate of z is denoted as (z_x, z_y). $f(z|g)$ shows the probability of the mechanism exposing z instead of g to a location-based service provider. $dis(a, b)$ denotes the Euclidian distance between two locations a and b. There are many obfuscation mechanisms being used in location privacy research, but most of them either are designed for cell-based frameworks, or consider the output location set Z the same as the actual location set G. Since we consider a more realistic framework in this thesis, we first show the LPPMs and the optimal remapping algorithm being used in Oya et al. [OTPG17a, OTPG17b], who consider continuous obfuscated locations like we do.

Uniform Circular Noise: Considering R to be the maximum radius of the circle, we sample the radius $r \in (0, R)$ following the probability density function $f(r) = \frac{r}{R^2}$, and sample the radian $\theta \in [0, 2\pi)$ using uniform distribution. $z_x = x + r * cos(\theta), z_y = y + sin(\theta)$.

Bi-dimensional Gaussian Noise: To generate Gaussian noise, we sample the noises in latitude and longitude dimensions Δx and Δy. Since Δx and Δy are independent, the probability density function is $f(\Delta x, \Delta y) = \frac{1}{2\pi\sigma_1\sigma_2} e^{-\frac{\Delta x^2}{2\sigma_1^2}-\frac{\Delta y^2}{2\sigma_2^2}}$. $z_x = x + \Delta x, z_y = y + \Delta y$.

Planar Laplace Noise: The planar Laplace mechanism is designed to achieve geo-indistinguishability [ABCP13]. We first uniformly sample p in the interval (0,1). Then set the radius of the Laplace noise $r = -\frac{1}{\epsilon}(W_{-1}(\frac{p-1}{e}) + 1)$, where W_{-1} is the -1 branch of the Lambert W function. We generate the radian θ by sampling uniformly in the interval $[0,2\pi)$. $z_x = x + r * cos(\theta), z_y = y + sin(\theta)$.

Exponential Mechanism: The exponential mechanism is a differential privacy technique that can achieve geo-indistinguishability [Dwo08]. We calculate the probability distribution function as $p(z|g) = a * e^{-b*dis(g,z)}$, where a guarantees $\sum_{z\in Z} p(z|g) = 1$.

Coin Mechanism: The coin mechanism [OTPG17a] is designed as an undesirable protection mechanism with an optimal average distance error. This mechanism outputs an actual location with probability α, and outputs a fake location $z*$ with probability $1 - \alpha$. We set $z^* = \arg\min_{z\in Z} \sum_{g\in G} \pi(g) dis(g, z)$, which is the geometric median of $\pi(g)$. Let the average quality loss $Q^* = \sum_{g\in G} \pi(g) dis(g, z^*)$. Then we build the probability distribution function as $f_{coin}(z|g) = \alpha * \delta(z - x) + (1 - \alpha) * \delta(z - z^*)$, where δ is the Dirac delta function. We set $\alpha = 1 - Q/Q^*$, where $Q \leq Q^*$ is the desired quality loss. Then the average distance error is Q.

Optimal Remapping: The optimal remapping method [CEP17] is used to minimize the average quality loss of a protection mechanism f. The remapping function is defined as $g(z'|z) = \delta(z' - r(z))$, where $r(z) = \arg\min_{z'\in Z} \sum_{g\in G} \pi(g) * f(z|g) * dis(x, z')$. The formula first calculates the minimal average distance error (the privacy metric), and then decreases the quality loss of the LPPM by remapping the fake location z to z', so that the quality loss is equal to the minimal average distance error. By doing so, the inferred location that an adversary chooses will always be z' in order to achieve the minimal average distance error. Then the protection mechanism with optimal remapping $f' = f \circ g$ can achieve optimality in terms of the average distance error privacy metric [OTPG17a].

Given the five LPPMs and the optimal remapping algorithm above, we will not use all of them in our experiments. For the uniform circular noise, due to us misunderstanding Oya et al.'s implementation of the uniform circular mechanism, we ended up not implementing it. We leave the implementation of this mechanism to future work.

The exponential mechanism is different from the other listed LPPMs because it only generates discrete outputs. The output set Z is the same as the actual location set G.

We also choose to ignore this LPPM for the following reasons. First, its performance is worse than planar Laplace noise in terms of geo-indistinguishability [OTPG17a]. Second, it cannot generate continuous outputs. Previous work [OTPG17a] used this LPPM to generated discrete outputs, and compared this LPPM with other LPPMs that generated continuous outputs. However, we think it is not appropriate to compare LPPMs some of which generate continuous outputs while some of which generate discrete outputs.

We will not use the coin mechanism in our experiment either, because the coin mechanism is designed to show that an undesired LPPM can also achieve an optimal average distance error. Thus, people should also use other metrics to distinguish such LPPMs. In our thesis, we only focus on evaluating how much location privacy users can protect with good LPPMs.

Optimal remapping is a useful algorithm to lower the quality loss of the LPPMs, in order to optimize the LPPMs by making the quality loss equal to the adversary's average distance error, when the adversary knows the users' entire mobility profiles. Our work mainly focuses on limited background knowledge and the success rate metric. Whether using optimal remapping or not will not affect our experiment results and our conclusions. Since adding the optimal remapping algorithm to our experiments will largely increase the run time, we remove the optimal remapping from our experiments.

Therefore, we use the bi-dimensional Gaussian noise and the planar Laplace noise in our experiments.

3.4 Metrics

To evaluate the tradeoff between utility and privacy, we need privacy metrics and quality loss metrics. Privacy metrics are used to distinguish whether an LPPM is good or bad given a certain quality loss. Average error is a standard privacy metric in location privacy. With different definitions of the function $d_{\chi}(g, g')$ in the metric, average error can be defined as either the average distance error, which is the average Euclidian distance between the adversary's inferred locations and actual locations, or the success rate, which is the rate of successfully inferred locations. We consider an adversary that is interested in either getting close to users' actual locations or inferring the actual locations. Thus, we use the average distance error and the success rate as our two privacy metrics.

Geo-indistinguishability [ABCP13] and conditional entropy [OTPG17a] are two complementary metrics to avoid undesirable LPPMs. The difference between these two metrics and the average error metrics is the former two metrics do not directly reflect what information an adversary can obtain from users' location records. Since our work focuses on quantifying location privacy by showing how much information an adversary can infer, we do not use these two metrics to evaluate our framework.

For quality loss metrics, we choose to calculate the average distance between the actual locations and obfuscated locations. The quality loss is determined by the configuration of the LPPM.

3.4.1 Average Error

The average error between the inferred locations and real locations is the most commonly used location privacy metric, but different researchers have different definitions for this metric.

Definition 1

$$\begin{aligned} P_{AE} &= \sum_{t \in T} \sum_{z \in Z} Pr(z) \sum_{g \in G} Pr(g|z) d_\chi(g', g) \text{ (where } g, g', z \text{ are generated in time period } t) \\ &= \sum_{t \in T} \sum_{z \in Z} \sum_{g \in G} K_G(g, t) Pr(z|g) d_\chi(g', g) \end{aligned}$$

where g, g', z represent the real location, inferred location, and observed location, respectively. $d_\chi(g', g)$ is an arbitrary distance function. For example, if we calculate the average distance error, $d_\chi(g', g) = dis(g', g)$ represents the Euclidean distance; if we calculate the success rate, $d_\chi(g', g) = c(g', g)$ is 1 when $g' = g$, or 0 otherwise. $\forall u \in U, t \in T, z \in Z$, if $d_\chi(g', g) = dis(g', g), g' = \arg\min_{g' \in G} \sum_{g \in G} Pr(g|z) dis(g', g)$; if $d_\chi(g', g) = c(g', g), g' = \arg\max_{g \in G} Pr(g|z)$.

Definition 1 is used in many recent papers, such as Oya et al. [OTPG17a] and Yu et al. [YLP17]. It theoretically minimizes the average error when the adversary accurately approximates the posterior probability distribution $Pr(g|z)$, that is, the adversary has enough background knowledge to construct K_G such that it is equal to users' mobility profiles. However, if the adversary is unable to obtain enough background knowledge and thus unable to accurately approximate the posterior probability distribution $Pr(g|z)$, then the average error may not be minimized.

Some previous papers [AHHH16,STD+11,STLBH11,STT+12] use another definition of average error:

Definition 2

$$\begin{aligned} P_{AE} &= \sum_{t \in T} Pr(z) P_{AE}(u,t) \\ &= \sum_{t \in T} Pr(z) \sum_{g' \in G} Pr(g'|z) d_{\chi}(g', g) \\ &= \sum_{t \in T} \sum_{g' \in G} K_G(g', t) Pr(z|g') d_{\chi}(g', g) \end{aligned}$$

where g, g', z are the real location, inferred location, and observed location, respectively at time t.

This definition of average distance error is based on the strategy that the adversary samples the inferred location following the probability distribution $Pr(g'|z)$ given an observed location z at time t. This definition does not minimize the average error as Definition 1 does. Though it looks reasonable, we have the following theorem:

Theorem 1 *Knowing the accurate posterior probability distribution $Pr(g|z)$ for all $g \in G$, the average error of using the strategy of choosing inferred location g' in Definition 2 will be larger than or equal to that of using the strategy in Definition 1.*

Proof *We assume $G = \{g_1, g_2, ..., g_n\}$, and denote $Pr(g_i|z) = p_i$, $i = 1, 2, ..., n$ given z, $\sum_{i=1}^{n} p_i = 1$. Without loss of generality, we assume $p_1 \geq p_2 \geq ... \geq p_n$.*

If we consider the metric as the average distance error metric, then $d_{\chi}(g', g) = dis(g', g)$. Let $g_k = \arg\min_{g' \in G} \sum_{j=1}^{n} p_j dis(g', g_j)$ in Definition 1. Let P_{AE1}, P_{AE2} be the average distance errors in Definition 1 and Definition 2 respectively. By sampling the inferred location following the probability distributions $Pr(g'|z)$ given z, we have:

$$
\begin{aligned}
P_{AE2} &= \sum_{j=1}^{n} p_j \sum_{i=1}^{n} p_i dis(g_i, g_j) \\
&= \sum_{i=1}^{n} p_i \sum_{j=1}^{n} p_j dis(g_i, g_j) \\
&\geq \sum_{i=1}^{n} p_i \sum_{j=1}^{n} p_j dis(g_k, g_j) \\
&= \sum_{j=1}^{n} p_j dis(g_k, g_j) \\
&= P_{AE1}
\end{aligned}
$$

If we consider the metric as success rate metric, then $d_\chi(g', g) = c(g', g)$. Let P_{SR1}, P_{SR2} be the success rates in Definition 1 and Definition 2 respectively. By sampling the inferred location following the probability distributions $Pr(g'|z)$, the probability of finding the real location is $\sum_{i=1}^{n} p_i^2$. By choosing g' with the highest $Pr(g'|z)$ as the inferred location, the probability is p_1. Then, we get:

$$
P_{SR2} = \sum_{i=1}^{n} p_i^2 \leq \sum_{i=1}^{n} p_i p_1 = p_1 = P_{SR1}.
$$

Thus, the average error of using the strategy of choosing inferred location g' in Definition 2 will be larger than or equal to that of using the strategy in Definition 1.

According to Theorem 1, we choose the metric and inference strategy in Definition 1 to evaluate the average error:

Average Distance Error: $P_{AE} = \sum_{t\in T} \sum_{z\in Z} Pr(z) \min\limits_{g'\in G} \sum_{g\in G} Pr(g|z) dis(g', g)$.

Success Rate: $P_{SR} = \sum_{t\in T} \sum_{z\in Z} Pr(z) \max\limits_{g'\in G} Pr(g'|z)$.

3.4.2 Quality Loss

The quality loss metric is usually defined as the average distance between the observed locations and the actual locations [STLBH11, YLP17, OTPG17a]. It is determined by the configuration of the LPPM. The definition is:

$$P_{QL} = \sum_{g \in G} \sum_{z \in Z} \pi(g) Pr(z|g) dis(g, z)$$

.

The quality loss metric is not only used to evaluate the utility loss, but also as an upper bound of the minimal error in terms of the average distance error metric, because an adversary can lower the average distance error to the quality loss by always choosing the observed location z (i.e., the output of an LPPM) as the inferred location g'. Furthermore, if we use optimal remapping to reduce the quality loss, then the quality loss of the optimized LPPM will be equal to the minimal average distance error. Therefore, if the average distance error of an attack is larger than the quality loss, we will know that this attack is not useful in terms of this metric, because there should be a smaller value for the average distance error.

3.5 Location Inference Attacks

Given an observed location z at time t, for all possible locations $g' \in G$, an adversary can try to infer the real location g based on the prior probability distribution of the LPPM $Pr(z|g')$, and the background knowledge about the user' mobility pattern $K_G(g', t)$ and $K_S(s', t)$. In this section, we introduce four different inference attacks with different combinations of the three parameters, targeting different privacy metrics.

3.5.1 Bayesian Inference Attack

The original Bayesian inference attack, called localization attack, was first proposed by Shokri et al. [STD+11]. Given the background knowledge $K_G(g', t)$, the probability of generating the fake location z $Pr(z)$, and the prior probability $Pr(z|g')$, this attack uses Bayesian inference to calculate the posterior probability $Pr(g'|z)$. The algorithm to infer the posterior probability distribution function $Pr(g'|z)$ is summarized in Algorithm 1. About how to choose the inferred location given the probability distribution $Pr(g'|z)$, different strategies are adopted for different privacy metrics. To minimize the average distance error metric, we choose the inferred location through traversing all $g' \in G$ as follows:

$$g' = \arg\min_{g' \in G} \sum_{g \in G} Pr(g|z) dis(g, g').$$

Algorithm 1: Original Localization Attack [STD+11]

```
Input: $Pr(z|g'), K_G(g', t)$
for $g' \in G$ do
    $Pr(g'|z) = \frac{Pr(z|g') * K_G(g', t)}{Pr(z)}$
end
Output: $Pr(g'|z)$.
```

Note that $Pr(g|z)$ is calculated using the user's mobility profile π_u. Since the adversary uses the background knowledge K_G^u to mimic π_u, he uses $Pr(g'|z)$ to approximate $Pr(g|z)$. When the adversary has complete background knowledge, $K_G^u = \pi_u$ and $Pr(g'|z) = Pr(g|z)$. To maximize the success rate, we choose the location with the highest posterior probability:

$$g' = \arg\max_{g' \in G} \sum_{g \in G} Pr(g|z)c(g, g') = \arg\max_{g' \in G} Pr(g'|z)$$

where $c(g, g') = 1$ if $g' = g$; otherwise $c(g, g') = 0$.

3.5.2 Bayesian Inference Attack with Extra Semantic Information

Usually only the prior probability $Pr(z|g')$ and geographical background knowledge $K_G(g', t)$ are considered when an adversary tries to infer users' actual locations. Agir et al. [AHHH16] show that semantic knowledge is very influential on geographical location privacy. However, one reason for which the semantic information becomes very useful is that the simplified cell-based framework without temporal properties loses a great part of geographical information. Agir et al. [AHHH16] partition San Francisco into only 96 cells. Each cell is about $1.25\,\text{km}^2$, which covers a large area. Therefore, any extra information such as semantic information can help a lot to build more accurate background knowledge of users. For example, if a user is a little more likely to be in cell 1 than in cell 2 given the geographical background knowledge, an adversary will guess the user is in cell 1. If the user is likely to be in a cinema given extra semantic information, and only cell 2 contains cinemas, then the user is actually more likely to be in cell 2 than cell 1.

In real life, users' locations are usually represented as points (i.e., coordinates), not large cells. If we assume the adversary has enough geographical background knowledge as what previous works do, the semantic background knowledge will not contain extra information for building better background knowledge, because the probability of a user visiting a semantic location is the sum of the probabilities of the user visiting every geographical location with this semantic tag. That is, if a location has a low probability of the geographical background knowledge, but its semantic tag has a high probability of the semantic background knowledge, the high semantic probability will not increase the possibility of the user going to this place. For instance, if a user does not like steaks and never goes to steak houses, even though the user often goes to restaurants, it does not mean the user will go to steak houses in the future. Agir et al. [AHHH16] use $Pr(g|s) * Pr(s)$ as the extra semantic information to calculate the inferred location. In our framework, however, it does not provide extra information because it is equal to the geographical background knowledge $Pr(g|s) * Pr(s) = Pr(g) = K_G$.

Although semantic information is no longer informative in terms of this formula, semantic information can still be useful in other ways. In reality the geographical background knowledge an adversary can obtain is usually limited. To decrease the impact of lacking enough knowledge, we can use semantic background knowledge as a complement. Our experiments in Chapter 4 will show that the semantic information has some impact on the attack results, though the impact is not as large as it is in Agir et al. [AHHH16].

We consider a scenario where a user goes to a new area, where no geographical background knowledge of this user is available, such as a user moves to a new city, or a user goes to a new restaurant that is in an area he never went to before. Since the user may still follow the similar semantic mobility patterns, such as often going to a bar at night, the adversary can still use the semantic background knowledge K_S from other areas instead of K_G to infer the user's locations. In the cases where the user goes to an area that he visited before, the adversary can still use the geographical background knowledge K_G to do Bayesian inference attack. This strategy is summarized in Algorithm 2. Besides this strategy, another way to consider semantic information in the attack by intuition is assigning 0.5 weight to both K_G and K_S and then adding them together. This strategy is summarized in Algorithm 3. This strategy will show that overestimating the impact of semantic information on the inference attack will make the attack performance even worse than not considering semantic information in the attack.

3.5.3 Background Knowledge Attack

Whether the Bayesian inference attack is successful or not relies on not only the amount of background knowledge, but also how much positive impact the prior probability distri-

Algorithm 2: Bayesian Inference Attack with Semantic Information 1

```
Input: $Pr(z|g'), K_G(g', t), K_S(s', t)$
if the adversary has background knowledge of this area then
    for $g' \in G$ do
        $Pr(g'|z) = \frac{Pr(z|g') * K_G(g',t)}{Pr(z)}$
    end
end
else
    for $g' \in G$ do
        $Pr(g'|z) = K_S(s', t)$ where $s'$ is the semantic tag of $g'$
    end
end
if use average distance error metric then
    Output: $\arg\min_{g' \in G} \sum_{g \in G} Pr(g|z)dis(g, g')$.
end
if use success rate metric then
    Output: $\arg\max_{g' \in G} Pr(g'|z)$.
end
```

bution $Pr(z|g)$ has on inferring actual locations. To evaluate the impact of the prior probability distribution of an LPPM on the attack results, we use the background knowledge attack that only uses geographical background knowledge to infer users' actual locations as a comparison. The background knowledge attack is described in Algorithm 4. Note that if an adversary only considers the background knowledge, ignoring the observed location z, then no matter where z is the inferred location will be the same. It will be the location g' that has the highest probability $K_G^u(g', t)$ in the time period t in the entire city. This may cause a large average error. Therefore, we use the obfuscated location z to draw a boundary of the 95% confidence interval such that an adversary can only consider the possible locations in the boundary area instead of the entire city. An adversary will consider the locations outside the boundary only if there is no location within the boundary. This step is done before running Algorithm 4.

Algorithm 3: Bayesian Inference Attack with Semantic Information 2

```
Input: $Pr(z|g'), K_G(g', t), K_S(s', t)$
for $g' \in G$ do
    $Pr(g'|z) = \frac{Pr(z|g')*(0.5*K_G(g',t)+0.5*K_S(s',t))}{Pr(z)}$
end
if use average distance error metric then
    Output: $\arg\min_{g' \in G} \sum_{g \in G} Pr(g|z)dis(g, g')$.
end
if use success rate metric then
    Output: $\arg\max_{g' \in G} Pr(g'|z)$.
end
```

Algorithm 4: Background Knowledge Attack with only Geographical Information

```
Input: $K_G(g', t)$
if use average distance error metric then
    Output: $\arg\min_{g' \in G} \sum_{g \in G} K_G(g, t)dis(g, g')$.
end
if use success rate metric then
    Output: $\arg\max_{g' \in G} K_G(g', t)$.
end
```

Chapter 4

Privacy Evaluation

The performance of attacks and defences are affected by each part of the framework. In this chapter, we design several experiments to quantify how much impact each part has on the framework. We will answer the following four questions:

- Does an adversary need a large amount of background knowledge to infer users' locations?
- How much impact does the prior probability distribution of a location privacy preserving mechanism have on inference attacks?
- Is an LPPM with the geo-indistinguishability property always better than an LPPM without this property?
- Do semantics have a large impact on inference attacks as people expect?

Our experiments are implemented using Python and C++ on a Ubuntu system. The implementation includes about 3000 lines of code in total. Although there are several open-source implementations of location privacy frameworks, they are not suitable for our framework. For example, the source code of Shokri et al. [STLBH11] is for cell-based frameworks with discrete fake locations; the source code of Oya et al. [OTPG17a] does not have an implementation of background knowledge construction, different attacks, and the success rate metric. Therefore, we run our experiments using our own implementation of the location privacy framework. Each experiment takes 2–6 hours, depending on how many attacks we need to run.

Note that the y axis of success rate graphs should have a range from 0 to 1. For the graphs in this chapter, since different lines in the figures are close to each other, showing the entire range [0,1] will make the lines indistinguishable from each other. Therefore, we omit part of the [0,1] range that no data point is in.

Due to lack of data (see Section 4.1), we have only 32 users to run our experiments. The small number of users and the variety of the users can cause large confidence intervals in our experiments. Especially, the 95% confidence intervals show the best cases and the worst cases in which the users are very predictable or very unpredictable. It is common to have large confidence intervals in location privacy research due to the various behaviours of different users. Since related work often only considers the average attack results over all users, we will also only consider the average attack results in our experiments. Due to the large confidence intervals, it is possible to generate different experimental results using different datasets. We draw our conclusions based on the average attack results using our dataset. The attack performance for each single user can be different.

4.1 Datasets

The users' location data we use in our experiments are from the check-in dataset built by Agir et al. [AHHH16]. The dataset contains public geo-tagged tweets in Twitter's public stream from 2014-01-01 to 2015-10-19. Each location record has semantic tags from a predefined list of categories in Foursquare [Fou18]. The original dataset contains check-in data from six cities. We choose the dataset in San Francisco since it contains the most data. Although there are several other popular location datasets (e.g., epfl/mobility dataset at CRAWDAD [PSDG09], Gowalla and Brightkite datasets [CML11]) for location privacy researchers, Agir et al.'s dataset [AHHH16] is the only one that has semantic tags for every location record.

In this datasest, we regard each location, such as a restaurant, a shop, a hospital, a road, as a PoI. No matter if a user is in the right corner or in the left corner of a restaurant, we consider this user is in the same location. Each PoI is assigned a location ID, and has at least one semantic tag. Since some PoIs have very specific semantic tags, such as "sushi restaurant", and others have more general semantic tags, such as "Japanese restaurant", or "food", we replace all semantic tags of the PoIs with the most general semantic tags in the category provided by Foursquare [Fou18]. The 11 semantic tags we use are "food", "nightlife spot", "arts & entertainment", "outdoors & recreation", "college & university", "event", "professional & other places", "residence", "shop & service", "travel & transport", and "unknown". We consider all 4597 locations appearing in the dataset as the set of PoIs

G, and select all 32 users with at least 500 location records in the dataset to use in our experiments.

Intuitively, we should partition the data into two parts. The first part is the historical data that are used to construct the adversary's background knowledge. The second part is regarded as the actual locations of users' current movements, which are used to test the location privacy frameworks. The shortcoming of this partition is it is hard to quantify the amount of background knowledge, because users' movements do not completely follow the mobility patterns based on previous location records. Also, although knowing users' entire mobility profiles is not realistic, researchers usually consider it as the worst case to calculate the minimal average distance error [STT+12,YLP17,OTPG17a]. Using this data partition method will make the adversary in location privacy research unable to achieve the minimal average distance error. Thus, we consider the same 500 location records to construct the adversary's background knowledge and to be the actual locations for testing. The adversary knows the users' entire mobility profiles when we use 500 locations per user to construct the background knowledge; the adversary knows the users' partial mobility profiles when we use from 1 to 499 locations per user to construct the background knowledge; the adversary knows nothing when we use 0 locations per user to construct the background knowledge.

4.2 The Impact of Adversary's Background Knowledge

Previous works usually assume a strong adversary who knows users' complete mobility profiles. In the real world, people may be confused about how much background knowledge is needed, since an adversary can hardly obtain the entire mobility profile of a user. In this section, we design an experiment to show the performance of inference attacks given different amounts of background knowledge.

The amount of background knowledge is evaluated as the number of locations that is used to construct the background knowledge. We choose the first k of the 500 location records for each user to construct different amounts of background knowledge. We vary the amount of location records k from 0 to 500. Each user has 500 actual location records for testing. We use two LPPMs, bi-dimensional Gaussian noise and planar Laplace noise, to evaluate two inference attacks, Bayesian inference attack and background knowledge attack, in terms of success rate metric. This experiment only takes geographical background knowledge into consideration. We ignore the experimental results in terms of average distance error metric, because no matter how much background knowledge an adversary has,

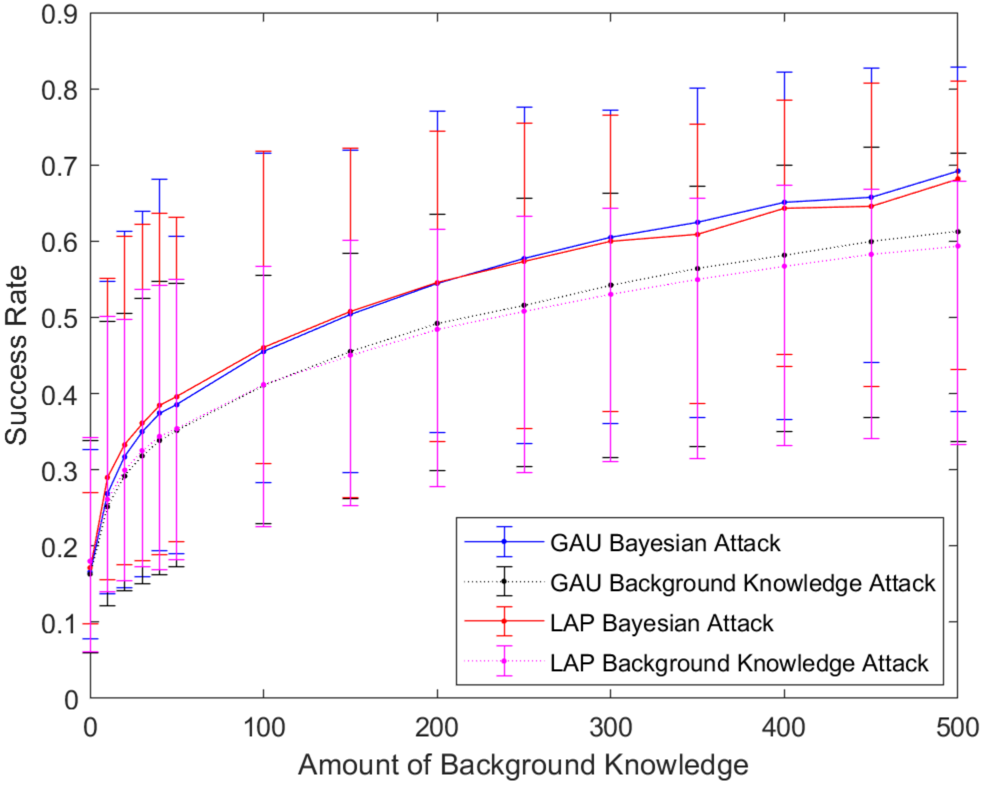

Figure 4.1: Evaluating Different Amounts of Background Knowledge with 0.1 km Quality Loss

the minimal average distance error for known attacks is always equal to the quality loss (see Section 3.4). One example will be described in Section 4.4, shown in Figure 4.4.

Figure 4.1, Figure 4.2, and Figure 4.3 show the success rates of the Bayesian inference attack and the background knowledge attack under different amounts of background knowledge and different quality losses. The labels "GAU" and "LAP" stand for bi-dimensional Gaussian noise and planar Laplace noise, respectively. The label "Bayesian attack" represents the original Bayesian inference attack in Algorithm 1; the label "Background knowledge attack" represents the attack in Algorithm 4 that only uses geographical background knowledge to infer users' actual locations. Besides, Figure 4.1 also shows the 95% confidence intervals. Since we only consider 32 users in our experiments, the 95% confidence intervals only indicate the best and the worst cases. The best cases show that a user has

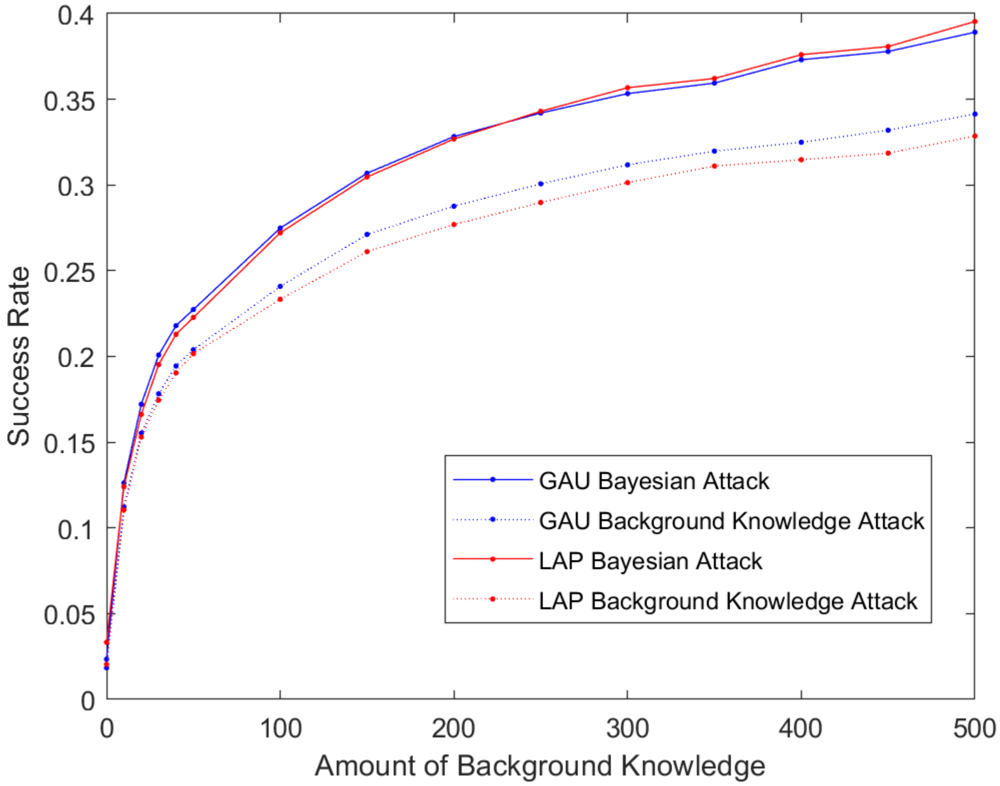

Figure 4.2: Evaluating Different Amounts of Background Knowledge with 0.5 km Quality Loss

very regular movements everyday, so it is very easy for an adversary to infer his actual locations. The worst cases show that a user has irregular movements everyday, so it is hard for an adversary to infer his actual locations even if the adversary has the complete background knowledge about this user. Therefore, the confidence intervals are large, which is very common in the location privacy research. Since we focus on the average attack results, in this thesis, we use this graph as an example, and do not show the confidence intervals in the other graphs. Intuitively, the number of actual locations that an adversary who only has a little background knowledge can infer is much smaller than the number of actual locations that an adversary who has full background knowledge can infer. However, according to the three figures, the success rates rocket at the beginning. This means, even only having a little background knowledge can significantly increase the success rate. Overall, an adversary only needs to obtain 6% of background knowledge to infer around 50%

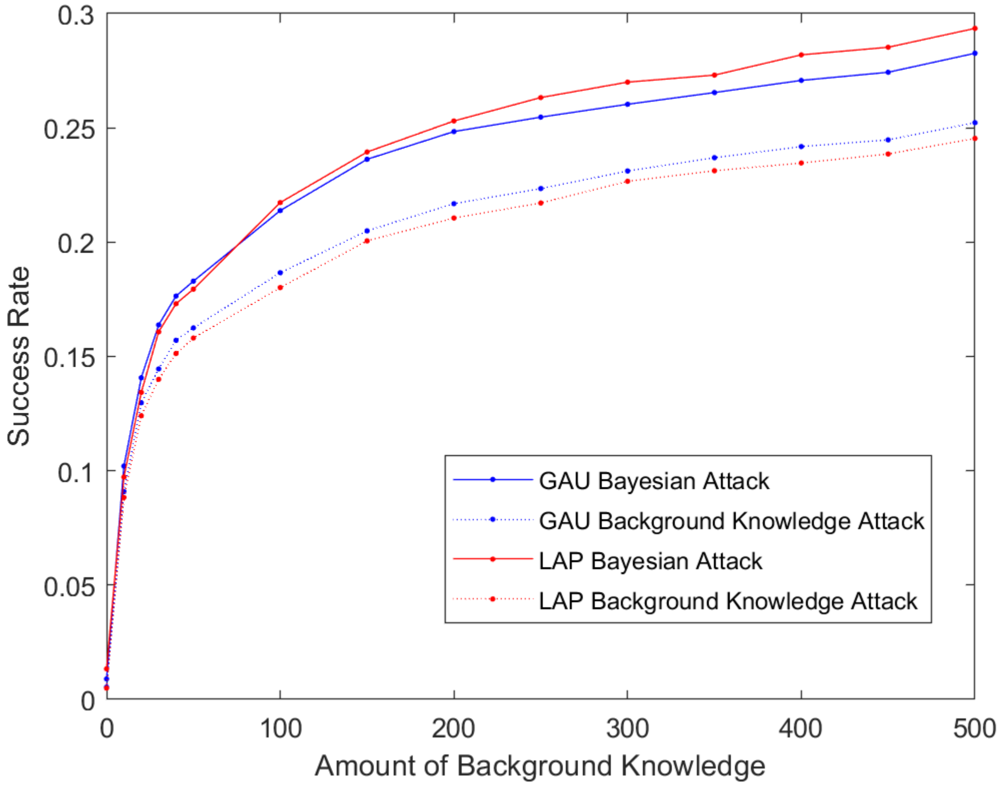

Figure 4.3: Evaluating Different Amounts of Background Knowledge with 1.0 km Quality Loss

of users' actual locations that he can infer when having full background knowledge. Even if an adversary obtains only 10 location records for each user to construct the background knowledge, he can infer a lot more users' locations than having no background knowledge. It also indicates that the users' behaviours do not change a lot during the two years. Besides, there are extreme cases of users. For one user most of whose check-in records are "home" and different "coffee shop", we can successfully infer more than 80% of his actual locations. For one user who goes to different restaurants and bars everyday, we can hardly infer his actual locations.

4.3 The Impact of the Prior Probability Distribution of an LPPM

The Bayesian inference attack is a good mathematical representation of location privacy threats. The background knowledge attack is an empirical attack to infer users' locations. The difference between the two attacks is that the Bayesian inference attack considers the prior probability distribution of the protection mechanisms. For example, if there exists an actual location g and a fake location z such that the prior probability $Pr(z|g)$ is significantly larger than the probabilities for other values of g, then it will be easy for an adversary to infer the actual location g given a fake location z with the prior probability distribution of the LPPM. However, a higher probability $Pr(z|g)$ does not always mean location g is more likely to be the actual location, given the observed fake location z. According to the user's mobility profile, the user may seldom or never visit location g. To evaluate how much impact the prior probability distribution of an LPPM has on inference attacks, we use the background knowledge attack as a comparison to assess the performance of Bayesian inference attacks.

It is true that the prior probability can have a large impact on the attack result given an undesirable LPPM, such as the coin mechanism. However, we are curious about the impact of $Pr(z|g)$ of good LPPMs (e.g., the bi-dimensional Gaussian noise, and the planar Laplace noise). According to Figure 4.1, Figure 4.2, and Figure 4.3, the prior probability $Pr(z|g)$ has some impact on the attack results, but the attack results are mainly determined by the background knowledge the adversary has, especially when the adversary does not have much background knowledge. Overall, no matter how much background knowledge an adversary has, the adversary can achieve more than 80% of the success rate that he can achieve when using the extra prior probability distribution of the LPPM. The reason is, a location that has a high prior probability may seldom or never be visited by the user, while a location with a high probability in geographical background knowledge is likely to be visited by the user even if the location does not have a high prior probability of the LPPM. The main impact of the prior probability distribution of the LPPM is to determine which location is more likely to be the real location, given all locations that have high probabilities in the geographical background knowledge.

4.4 The Impact of Geo-indistinguishability

The geo-indistinguishability metric is used to evaluate how informative the prior probability distribution $Pr(z|g)$ is. Ideally, if an LPPM achieves a higher privacy level of

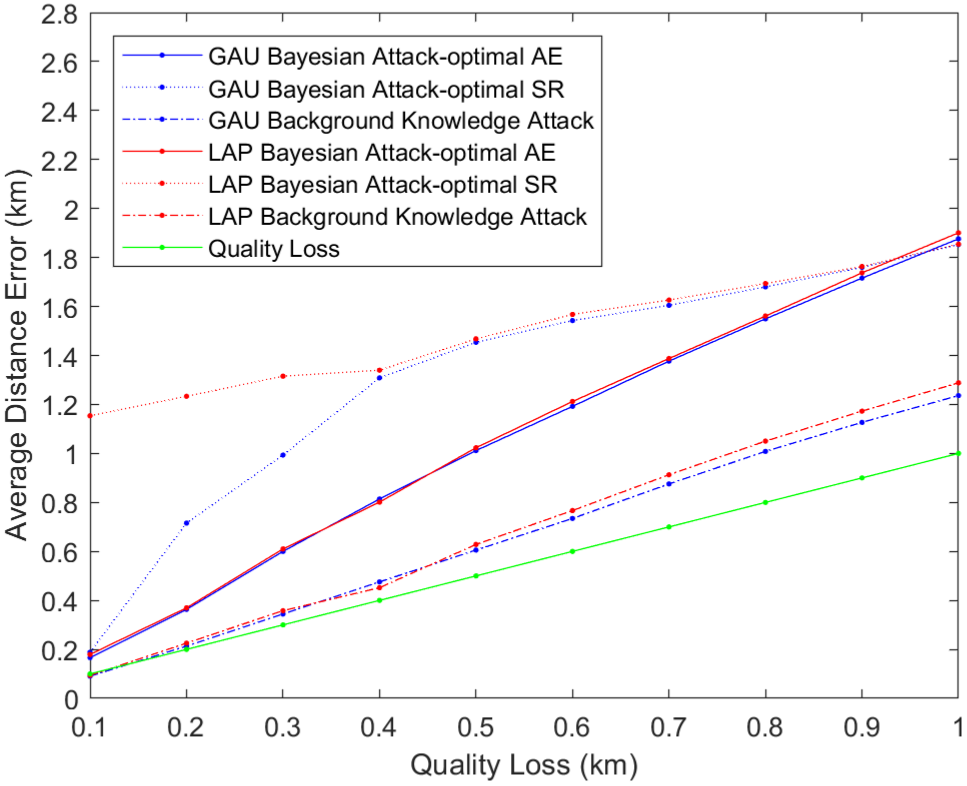

Figure 4.4: Evaluating Different LPPMs in Terms of Average Distance Error with No Background Knowledge

geo-indistinguishability, it becomes harder for an adversary to infer a user's location information without background knowledge. Since Section 4.3 shows that the prior probability distribution has minor impact on the attack results, this may mislead the designers of LPPMs to blindly improve the privacy level of geo-indistinguishability but get little effect on the attack results. In this section, we design an experiment to show that an LPPM that has the geo-indistinguishability property is not always better than other LPPMs.

Planar Laplace noise is designed to guarantee the geo-indistinguishability property, while bi-dimensional Gaussian noise is not. We evaluate the two LPPMs in terms of geo-indistinguishability against an adversary with no background knowledge. The attack performances with different quality losses are shown in Figure 4.4 and Figure 4.5.

Figure 4.4 shows the attack results in terms of the average distance error metric. Since

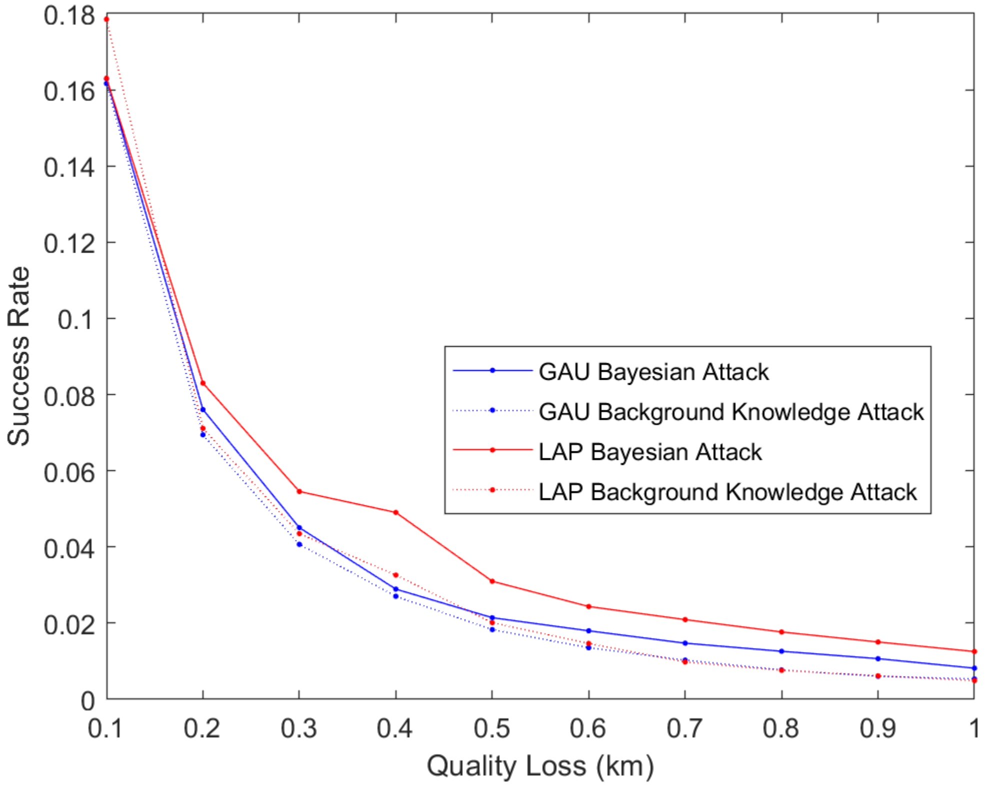

Figure 4.5: Evaluating Different LPPMs in Terms of Success Rate with No Background Knowledge

the geo-indistinguishability property is isolated from users' background knowledge, we assume the adversary has no background knowledge in this experiment. If the adversary knows the entire users' mobility profiles, given the posterior probability distribution $Pr(g|z)$, we have two strategies of choosing the best inferred locations. As described in Section 3.5, the first strategy is to minimize the average distance errors, and the second is to maximize the success rates. However, it is unsure which strategy is better when the adversary has no background knowledge. Therefore, we use both of the two strategies in this figure, labeled as "Bayesian Attack-optimal AE", and "Bayesian Attack-optimal SR". Also, similar to our other experiments, we use the background knowledge attack with optimal success rate strategy as a comparison. The corresponding label in the figure is "Background Knowledge attack". In addition, choosing the observed fake location as the inferred location is another strategy to achieve an average distance error equal to the quality loss, labeled as "Quality Loss". This implies that the quality loss is an upper bound of the minimal average distance error. Figure 4.4 shows that in most of the cases, the Gaussian noise mechanism and the Laplace noise mechanism have very similar performance. When the quality loss is less than 0.4 km, the Laplace noise causes a significantly larger average distance error than the Gaussian noise does, but the average distance errors of both of them are much larger than the quality loss. This means, if an unsophisticated adversary does not know about the background knowledge attack or how to minimize the distance error to the quality loss, and can only use the Bayesian inference attack, then the Laplace noise with the geo-indistinguishability property can better protect users' location privacy in terms of average distance error metric. However, in location privacy research we cannot only assume an unsophisticated attacker. If an adversary knows all attack strategies, using Laplace noise with the geo-indistinguishability property is not better than using Gaussian noise without this property, since the known minimal average distance error is always equal to the quality loss.

Figure 4.5 shows the attack results without any background knowledge in terms of the success rate metric. The meanings of the labels in this figure is the same as those in previous figures. All the attacks are using the optimal strategy to maximize the success rate. According to this figure, the adversary can achieve a higher success rate when the users use the Laplace noise mechanism. This indicates the Laplace noise, which has the geo-indistinguishability property, is a little more vulnerable than Gaussian noise in our experiment.

As a conclusion, people should not blindly rely on or improve the geo-indistinguishability property when designing LPPMs. Although geo-indistinguishability can filter the badly designed mechanisms (e.g., the coin mechanism), for good mechanisms (e.g., Gaussian noise, Laplace noise, etc.), improving their geo-indistinguishability property does not necessarily improve the performance of the LPPM against existing attacks.

4.5 The Impact of Semantic Background Knowledge

Besides the coordinates of users' locations (i.e., geographical information), semantic information is another available type of background knowledge that can be used to infer users' locations. Agir et al. [AHHH16] show semantic information has a significant impact on the inference attack performance when considering a simplified cell-based framework against simplified attacks. If the framework is not simplified, however, the performance can be different. As explained in Chapter 3, when considering each PoI as a location instead of

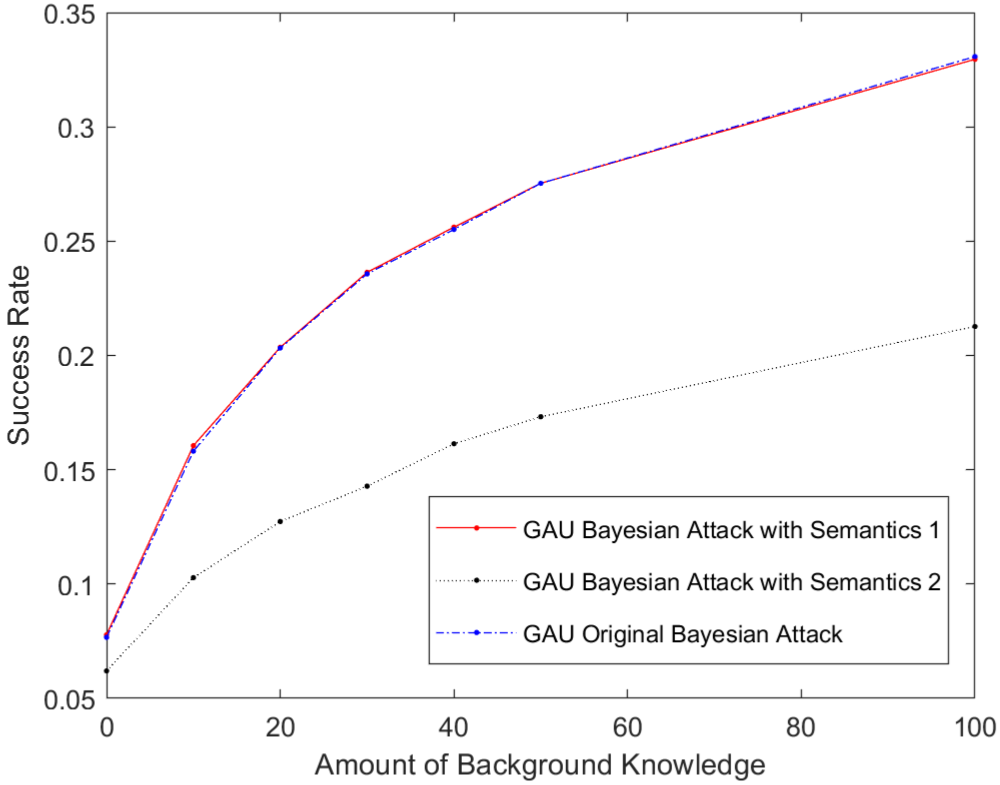

Figure 4.6: Evaluating Bayesian Inference Attacks With/Without Semantic Background Knowledge

using a cell-based framework, the semantic information will not contain extra information when the attacker has much geographical background knowledge in the area. Semantic information can still be useful when the user is moving within a new area where he never went to before. Because we are unable to find an available dataset that contains location records of more than one city for each user, we decide to seek a compromise. In this experiment, we only allow the adversary to have a little background knowledge, and also decrease the quality loss of the LPPMs, in order to create some areas that the users never went to before (i.e., the background knowledge does not contain location records in these areas), but will be here in the future (i.e., the users' actual locations for testing contain location records in these areas).

Figure 4.6 shows the attack results using the bi-dimensional Gaussian noise mechanism against different inference attacks with or without semantic information. The quality loss is 0.2 km. Adding extra semantic information to the attacks aims at inferring more actual locations, so we only consider the success rate metric in this experiment. We ignore the average distance error metric also because the minimal error is always equal to the quality loss in this experiment. In this figure, the label "GAU Bayesian Attack with Semantics 1" represents the attack in Algorithm 2, which considers semantic background knowledge only when a user is in a new area. The label "GAU Bayesian Attack with Semantics 2" represents the attack in Algorithm 3, which considers both the geographical knowledge and the semantic knowledge with 0.5 weights respectively in all situations. The label "GAU Original Bayesian Attack" represents the attack in Algorithm 1, which only considers the geographical background knowledge in the Bayesian inference attack. According to Figure 4.6, the graph of Bayesian inference attack with semantics in Algorithm 2 overlaps with the graph of the attack without semantics when we use fewer than 50 location records to construct the background knowledge. Because we only allow the adversary to have a very little background knowledge in order to create some new places that the users will go to, the lack of background knowledge significantly affects the attack performance. Therefore, we are unable to show how useful the semantic information can be in the situation that a user goes to a new place. In future work, we will try to process the dataset we have to make it suitable for this experiment, and show the impact of semantic information on the attack results. In addition, the semantic attack in Algorithm 3 has much worse performance than the other two attacks. This is because for the locations that the user seldom or never goes to, but have a semantic tag with a high probability in semantic background knowledge, adding semantic information into the Bayesian inference attack misleads the adversary. For example, a user may go to restaurants very often, but never goes to pizza restaurants. In this case, a pizza restaurant should have a low posterior probability, but the probability can increase a lot if we add the high probability of the "restaurant" semantic tag to the pizza restaurant.

4.6 Conclusion

In this chapter, we show that different parts of the location privacy framework have different impacts on the attack results, which may be different from people's intuition. An adversary's ability to infer users' actual locations can be significantly improved by obtaining a little geographical background knowledge of the users. The prior probability distribution of an LPPM is relatively less influential than the geographical background knowledge. The semantic background knowledge is less useful to the adversary than what previous papers show, but it can help the adversary to infer a user's locations when the user is in a new area (e.g., the user moves to a new city). An LPPM with the geo-indistinguishability property is not always better than LPPMs without this property. We should not blindly rely on geo-indistinguishability when evaluating or designing LPPMs.

Chapter 5

Future Work

In this chapter, we list some possible future work.

Location Datasets

In our evaluation, we only use the check-in data from San Francisco. Agir et al. [AHHH16] show that there is no major difference among the six different cities in the check-in dataset in terms of user privacy. Since the check-in data we have are all from big cities, we can also try to create and test datasets from different areas, such as urban areas and rural areas, to compare the differences of different areas.

Background Knowledge

Instead of only varying the amounts of users' background knowledge an adversary has, we can also test different time partitions, and different classifications of semantic information. For time partitions, for example, we can partition a week into work days and weekends, or partition a year into common days and holidays. For semantic classifications, we can use more specific semantic tags, such as "movie theater" and "Italian restaurant", instead of general semantic tags, such as "arts & entertainment" and "food".

LPPMs

A possible future work is evaluating more LPPMs. Many LPPMs have been proposed in previous papers, but since they are using the cell-based framework, the LPPMs only allow discrete inputs and outputs. How to change the algorithms of the LPPMs to allow the LPPMs to evaluate continuous location inputs and outputs can be future work. By doing so, we can further compare the performance of other LPPMs, to know more about the different behaviours of different LPPMs.

Metrics

Conditional entropy [OTPG17a] is another metric that has been considered useful recently; however, previous papers [OTPG17a] only use an undesirable LPPM, the coin mechanism, to show different LPPMs have different conditional entropy. It is unknown how much impact the conditional entropy metric has on evaluating LPPMs, given more LPPMs.

Chapter 6

Conclusion

In this thesis, we introduce our location privacy framework, and then use this framework to quantify users' location privacy from an adversary's point of view. The experimental results show different parts of the location privacy framework have different impacts on attack performance, indicating the limitations of how much we can improve these parts. To be specific, geographical background knowledge has a very large impact on the attack results. An adversary only needs to obtain 6% of background knowledge to infer around 50% of users actual locations that he can infer when having full background knowledge. The semantic background knowledge, however, is not as useful as claimed in previous papers. Semantic information is not informative in most of the cases, but can help an adversary to infer a user's locations when the user moves around in a new area that he has never gone to. For the prior probability distribution of an LPPM, although it can be used in the inference attacks, the attack results are mainly determined by the amount of background knowledge an adversary has. Our experiments show that no matter how much background knowledge the adversary has, the adversary can achieve overall 80% of the success rate that he can achieve when also using the prior probability distribution of the LPPM in the attack. In addition, our evaluation of the geo-indistinguishability metric indicates that a good LPPM with the geo-indistinguishability property is not always better than a good LPPM without this property, though some undesirable LPPMs can be distinguished by geo-indistinguishability. In conclusion, we believe our findings will help users and researchers have a better understanding of location privacy attacks and defences in our more realistic framework. For example, people should not blindly believe that an LPPM with geo-indistinguishability is better. Also, since the attack results are mainly determined by the background knowledge, we suggest people focus more on how to defend against the background knowledge attack, instead of focusing on how to make the prior probability of an LPPM more indistinguishable. One of the possible proposals is combining the mechanisms of adding dummy locations and generating noises. In addition, people can further study the impact of semantic information, since the impact of semantic information in our more realistic framework can be different from that in a cell-based framework.

References

[ABCP13] Miguel E Andrés, Nicolás E Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, pages 901–914. ACM, 2013.

[AHHH16] Berker Ağır, Kévin Huguenin, Urs Hengartner, and Jean-Pierre Hubaux. On the privacy implications of location semantics. *Proceedings on Privacy Enhancing Technologies*, 2016(4):165–183, 2016.

[BCP14] Nicolás E Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Optimal geo-indistinguishable mechanisms for location privacy. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 251–262. ACM, 2014.

[BWJ05] Claudio Bettini, X Sean Wang, and Sushil Jajodia. Protecting privacy against location-based personal identification. In *Workshop on Secure Data Management*, pages 185–199. Springer, 2005.

[CABP13] Konstantinos Chatzikokolakis, Miguel E Andrés, Nicolás Emilio Bordenabe, and Catuscia Palamidessi. Broadening the scope of differential privacy using metrics. In *Privacy Enhancing Technologies Symposium*, pages 82–102. Springer, 2013.

[CEP17] Konstantinos Chatzikokolakis, Ehab ElSalamouny, and Catuscia Palamidessi. Practical mechanisms for location privacy. *Proceedings on Privacy Enhancing Technologies*, 4:210–231, 2017.

[CML11] Eunjoon Cho, Seth A Myers, and Jure Leskovec. Friendship and mobility: User movement in location-based social networks. In *Proceedings of the 17th*

ACM SIGKDD international conference on Knowledge discovery and data mining, pages 1082–1090. ACM, 2011.

[CPS15] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Marco Stronati. Constructing elastic distinguishability metrics for location privacy. *Proceedings on Privacy Enhancing Technologies*, 2015(2):156–170, 2015.

[CSPE12] Bogdan Carbunar, Radu Sion, Rahul Potharaju, and Moussa Ehsan. The shy mayor: Private badges in geosocial networks. In *International Conference on Applied Cryptography and Network Security*, pages 436–454. Springer, 2012.

[DBS+10] Maria Luisa Damiani, Elisa Bertino, Claudio Silvestri, et al. The probe framework for the personalized cloaking of private locations. *Trans. Data Privacy*, 3(2):123–148, 2010.

[DD11] Changyu Dong and Naranker Dulay. Longitude: A privacy-preserving location sharing protocol for mobile applications. In *IFIP International Conference on Trust Management*, pages 133–148. Springer, 2011.

[DK05] Matt Duckham and Lars Kulik. A formal model of obfuscation and negotiation for location privacy. In *International conference on pervasive computing*, pages 152–170. Springer, 2005.

[Dwo06] Cynthia Dwork. Differential privacy. In *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ICALP'06, pages 1–12, Berlin, Heidelberg, 2006. Springer-Verlag.

[Dwo08] Cynthia Dwork. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pages 1–19. Springer, 2008.

[Fou18] Foursquare. URL: https://developer.foursquare.com/docs/resources/categories/, 2018. (visited on 05/2018).

[FS14] Kassem Fawaz and Kang G Shin. Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 239–250. ACM, 2014.

[GG03] 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.

[GH05] Marco Gruteser and Baik Hoh. On the anonymity of periodic location samples. In *International Conference on Security in Pervasive Computing*, pages 179–192. Springer, 2005.

[GL08] Bugra Gedik and Ling Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, 2008.

[GP09] Philippe Golle and Kurt Partridge. On the anonymity of home/work location pairs. In *International Conference on Pervasive Computing*, pages 390–397. Springer, 2009.

[HRDP14] Michael Herrmann, Alfredo Rial, Claudia Diaz, and Bart Preneel. Practical privacy-preserving location-sharing based services with aggregate statistics. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pages 87–98. ACM, 2014.

[KFS15] Huan Feng Kassem Fawaz and Kang G Shin. Anatomization and protection of mobile apps' location privacy threats. In *24th USENIX Security Symposium, Jaeyeon Jung and Thorsten Holz (Eds.). USENIX Association*, pages 753–768, 2015.

[Kru09] John Krumm. Realistic driving trips for location privacy. In *International Conference on Pervasive Computing*, pages 25–41. Springer, 2009.

[LLV07] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*, pages 106–115. IEEE, 2007.

[MC14] Changsha Ma and Chang Wen Chen. Nearby friend discovery with geo-indistinguishability to stalkers. *Procedia Computer Science*, 34:352–359, 2014.

[MGBF14] Benjamin Mood, Debayan Gupta, Kevin Butler, and Joan Feigenbaum. Reuse it or lose it: More efficient secure computation through reuse of encrypted values. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 582–596. ACM, 2014.

[MGKV06] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. In *International Conference on Data Engineering*, pages 24–24, 2006.

[OTPG17a] 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.

[OTPG17b] 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.

[PS11] Sai Teja Peddinti and Nitesh Saxena. On the limitations of query obfuscation techniques for location privacy. In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 187–196. ACM, 2011.

[PSDG09] 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.

[PTDC17] Apostolos Pyrgelis, Carmela Troncoso, and Emiliano De Cristofaro. What does the crowd say about you? evaluating aggregation-based location privacy. *Proceedings on Privacy Enhancing Technologies*, 2017(4):156–176, 2017.

[SGI09] Pravin Shankar, Vinod Ganapathy, and Liviu Iftode. Privately querying location-based services with sybilquery. In *Proceedings of the 11th international conference on Ubiquitous computing*, pages 31–40. ACM, 2009.

[Sho15] Reza Shokri. Privacy games: Optimal user-centric data obfuscation. *Proceedings on Privacy Enhancing Technologies*, 2015(2):299–315, 2015.

[STD$^+$11] Reza Shokri, George Theodorakopoulos, George Danezis, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Quantifying location privacy: The case of sporadic location exposure. In *Privacy Enhancing Technologies Symposium*, pages 57–76. Springer, 2011.

[STLBH11] 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.

[STT$^+$12] 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.

[Swe02] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[WSDR14] 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.

[XC09] Toby Xu and Ying Cai. Feeling-based location privacy protection for location-based services. In *Proceedings of the 2009 ACM Conference on Computer and Communications Security*, pages 348–357. ACM, 2009.

[XKP09] Mingqiang Xue, Panos Kalnis, and Hung Keng Pung. Location diversity: Enhanced privacy protection in location-based services. In *International Symposium on Location-and Context-Awareness*, pages 70–87. Springer, 2009.

[XXM08] Zhen Xiao, Jianliang Xu, and Xiaofeng Meng. p-sensitivity: A semantic privacy-protection model for location-based services. In *Mobile Data Management Workshops, 2008. MDMW 2008. Ninth International Conference on*, pages 47–54. IEEE, 2008.

[YLP17] Lei Yu, Ling Liu, and Calton Pu. Dynamic differential location privacy with personalized error bounds. In *The Network and Distributed System Security Symposium*, 2017.

[ZB11] Hui Zang and Jean Bolot. Anonymization of location data does not work: A large-scale measurement study. In *Proceedings of the 17th annual international conference on Mobile computing and networking*, pages 145–156. ACM, 2011.

[ZGH07] Ge Zhong, Ian Goldberg, and Urs Hengartner. Louis, Lester and Pierre: Three protocols for location privacy. In *International Workshop on Privacy Enhancing Technologies*, pages 62–76. Springer, 2007.