Companion Technical Report for SFERA a toolkit for Assessing Location Privacy with Re-Identification Attacks

Mohamed Maouche
INSA Lyon - LIRIS, Lyon, France
mohamed.maouche@insa-lyon.fr

Sonia Ben Mokhtar
CNRS - LIRIS, Lyon, France
sonia.benmokhtar@insa-lyon.fr

Sara Bouchenak INSA Lyon - LIRIS, Lyon, France
sara.bouchenak@insa-lyon.fr

April 25, 2017

Abstract

Since the advent of hand held devices (e.g., smartphones, tablets, smart watches) and the wide popularity of location-based mobile applications, the amount of captured user location data is increasing. However, the gathering and exploitation of this data by mobile application providers raises many privacy threats as sensitive information can be inferred from it (e.g., home and work locations, religious beliefs, sexual orientations and social relationships). To address this issue a number of data obfuscation techniques (also called Location Privacy Protection Mechanisms or LPPMs) have been proposed in the literature. However, it is difficult for the designers of such mechanisms to assess their effectiveness in practice. In this paper we propose SFERA, a novel toolkit for assessing the degree of protection offered by a given LPPM to end users, using re-identification attacks. The aim of these attacks is to break user anonymity by re-associating their obfuscated data with profiles built from their past mobility. Our toolkit includes two state-of-the-art attacks in addition to AP-Attack a novel re-identification attack that relies on a heatmap representation of user mobility data. We demonstrate the effectiveness of our toolkit by providing a thorough evaluation of three representative LPPMs of the literature using four real mobility datasets and a demonstration on how the toolkit can be used to obfuscate a dataset with user-centric multi-LPPM protection.

1 Introduction

With the raising number of mobile devices and the wide popularity of mobile applications, an increasing amount of mobility data is being gathered, processed and sometimes sold to third parties by application providers due to their inherent economic model. Examples of such applications include GPS navigation (e.g., GoogleMaps [1], Waze), location-based social networks (e.g., Swarm with Foursquare [2] or geo-gaming (e.g., Pokemon GO [3]). At the same time, following the open data movement, major socio-economic actors (e.g., telecommunication companies) and local authorities (e.g., cities) are pushed to give back their data to the society by publishing the datasets they are collecting about individuals [4, 5, 6]. However, as shown in various studies, the publication of user mobility data opens a number of privacy threats [7] [8] [9]. For instance, one can extract particular places where users regularly stop, also called Points Of Interest (POI) [10], like the user's home location, work place [11], places of worship [12] or even discover the user health status if she regularly goes to the hospital. Moreover, by analyzing POIs of different users, social relationship can be discovered [13] and labels such as : siblings, colleagues, significant others. . . , can be associated to these relations.

To deal with this issue, various location privacy protection mechanisms (also called LPPMs) have been devised to protect the privacy of users when their mobility data is shared with applications. These mechanisms can be classified according to two usage scenarios. The first scenario, called the *online scenario* applies when users send their GPS coordinates to an application provider in order to get a geo-localized response (e.g., finding a restaurant in the user's vicinity, GPS navigation). In this context the LPPM, which runs on the client side can only act on the GPS coordinates sent by the user at a given time and place. Examples of such LPPMs include *Geo-Indistinguishablility* [14], where Laplacian noise is added to each GPS coordinate, *CloakDroid* [15], where the GPS data is discretized using a grid or *Android Location Privacy Framework* [16], where various obfuscation techniques can be applied such as the generalization of a given location to the closest street, city, postal code and more. The second scenario, called the *offline scenario* applies when a given service provider collects a mobility dataset and needs obfuscation techniques to protect the participating users' privacy before releasing the dataset. In this context, the LPPM, which runs on the server side, has a broader view of the mobility of the overall population of users and can thus apply more sophisticated obfuscation techniques. Examples of such LPPMs include *GLOVE* [17], where mobility traces are merged together using a spatio-temporal similarity metric, *Never Walk Alone* [18] and its extension *W4M* [19], where cylindrical volumes wrap the movement of at least k different users together.

However, in both the online and the offline cases it is difficult to assess the effectiveness of the proposed LPPMs in practice. Indeed, LPPMs are generally evaluated either theoretically by proving the guarantees they offer to the users (e.g., k-anonymity [20] or differential privacy [21]) or practically by using custom privacy metrics that are often difficult to interpret, such as in [22] where POI

retrieval metric is used to quantify privacy. Indeed, it is difficult to tell a data owner that aims at obfuscating her dataset whether obfuscating her dataset by enforcing k-anonymity with the *W4M* protocol [19] is better than obfuscating it by enforcing differential privacy with the *Geo-Indistinguishablility* protocol [14]. To help answering this question, the approach we propose in this paper is to rely on user re-identification attacks. Considering an obfuscated mobility dataset and a set of user profiles learnt from users past mobility, a user re-identification attack tries to re-associate a portion of obfuscated data to its originating user. It is worth mentioning that the terminology *de-anonymization* can be found in place of *re-identification* (e.g., [24]). We would rather use de-anonymization to describe the process of finding a user real identity (e.g., name, address...) while re-identification describe the process of finding a user ID in the system. Literature contains a number of user re-identification attacks. These attacks can be distinguished according to two key elements: the user profiles they build from users past mobility and the distance metric they use to compare obfuscated data with user profiles. The most representative attacks proposed in the literature are POI-Attack [23] and PIT-Attack [24]. In the former, a user profile is represented by the list of POIs visited by the user while in the latter a user profile is represented by a Markov chain between the POIs visited by the user. However, none of these attacks consider the past mobility of users as a whole (i.e., considering both the places where the users stop and the trajectories that lead to these places).

In this paper, we first present AP-Attack a novel attack in which a user profile is represented as a heat-map. We compare the performance of AP-Attack to the two above attacks on four real mobility datasets and show that AP-Attack succeeds in re-identifying up to +27% more users than POI-Attack and up to +34% more users than PIT-Attack.

We further integrate AP-Attack in a toolkit called SFERA. The aim of this toolkit is two fold: (1) helping a system designer to study the resilience of her LPPM to powerful re-identification attacks including our own attack in addition to state-of-the-art attacks and (2) helping data owners in the difficult task of obfuscating their datasets. We demonstrate the usefulness of SFERA through two use cases. Our first use case analyses the ability of three state-of-the-art LPPMs (i.e., Geo-I [14], Promesse [22] and W4M [19]) to protect the users of four real datasets against the attacks integrated in SFERA. Results show that none of the studied LPPMs succeeds in protecting all the users. Our second use case studies the vulnerability of individual users to re-identification attacks when their data is obfuscated using the above three LPPMs. Results show that users are not equal in front of re-identification attacks, some can not be protected by the considered LPPMs, some are naturally protected against the attacks, while others can be protected by one or multiple LPPMs. Using this observation, that to the best of our knowledge we are the first to establish, we propose a Multi-LPPM user-centric obfuscation technique, which outperforms all the evaluated LPPMs.

The remaining of this paper is structured as follows. First, we present in Section 2, a background on location privacy. Then, we present in Section 3 a

model for re-identification attacks included in SFERA as well as the instantiation of this model for two state-of-the-art attacks before presenting AP-Attack a new re-identification attack in Section 4. Further, we present our SFERA toolkit in Section 5 and its evaluation in Section 6. Finally we describe related research works in Section 7 before concluding the paper in Section 8

2 Background and System Model

We present in this section a set of background definitions related to mobility traces (Section 2.1) and to location privacy protection mechanisms (Section 2.2).

2.1 Mobility Traces

A mobility trace is constituted of a sequence of spatio-temporal points (lat, lng, t) associated to a given user, where lat and lng correspond to the latitude and longitude of GPS coordinates while t is a time stamp. The top part of Figure 1 shows a visual representation of a mobility trace (spacial elements only) of a given user collected in the city of San Fransisco.

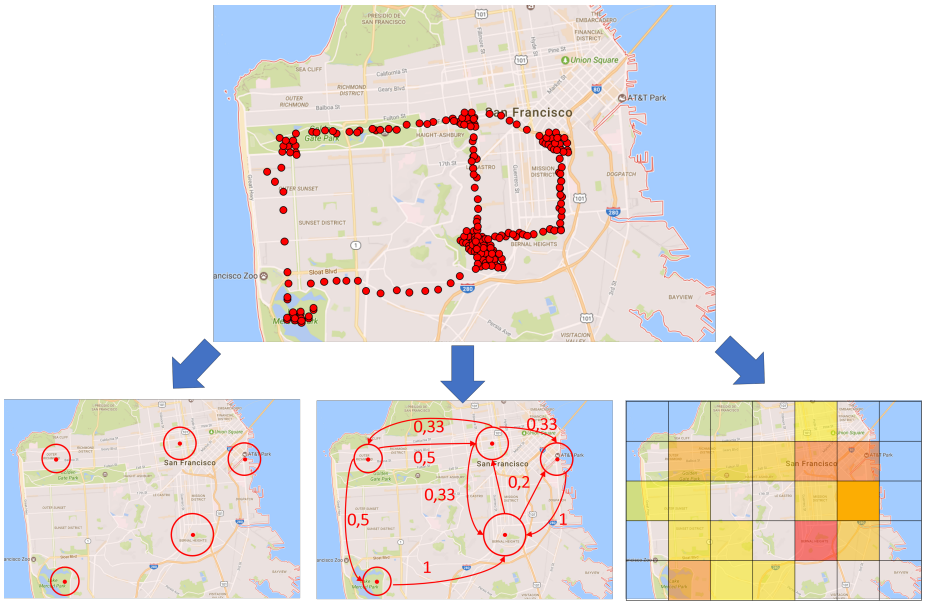
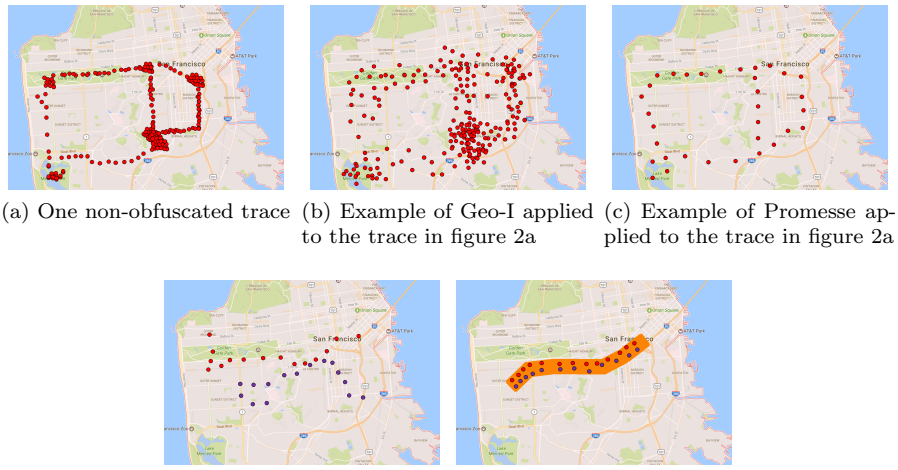


Figure 1: Various representations of mobility traces

In order to associate semantic information to user raw mobility traces, various mobility models can be built from these traces. The bottom part of Figure 1 shows examples of such models. In this figure, the left part represents a mobility model in which only user points of interest (POIs) have been extracted.



(a) One non-obfuscated trace (b) Example of Geo-I applied to the trace in figure 2a (c) Example of Promesse applied to the trace in figure 2a

(d) Two non-obfuscated traces (e) Example of W4M applied to the traces in figure 2d

Figure 2: Example of LPPMs applied to mobility traces

POIs are particular places where a user has stopped for a given amount of time. They are extracted from raw traces using spatio-temporal clustering algorithms such as [25, 26]. POIs may reveal personal information such as a user's home place, work place or even sexual orientation and religious beliefs. The central part of the figure represents a mobility model in the form of a Markov chain between user POIs. This model is richer than the former one as it captures user mobility habits between POIs (e.g., the probability that the user goes to her favorite Japanese restaurant after going to the movie theatre). Finally, the right part of the figure represents a mobility model in which the map has been split into cells and the raw data has been projected into these cells in the form of a heat-map. Specifically, in this model, the intensity of the color of a given cell is relative to the frequency of user visits in the corresponding area of the map. Even though this model does not convey detailed temporal information about the user mobility, it is the only one to capture information about user trajectories. We will later use this model to build a novel user re-identification attack presented in Section 4.

2.2 Location Privacy Protection Mechanisms - LPPMs

To overcome the threats affecting location privacy, Location Privacy Protection mechanisms (LPPMs) have been proposed in the literature. LPPMs generally take as input a mobility trace (sometimes composed of a single record) or a set of mobility traces and alter these traces in order to produce obfuscated traces. LPPMs can be used in an online fashion, where each record is obfuscated before

being sent to an application provider, or offline, where all the traces will be obfuscated at once. Furthermore, LPPMs are often classified depending on the privacy guarantees they offer to the users. There exist two major privacy guarantees presented in the literature: k-anonymity [20] and differential privacy [21]. The k-anonymity property states that a user is hidden among a set of $k-1$ other users with similar properties. In the context of mobility data this translates to the ability to hide a given user in a geographical zone (called a cloaking area) where there are at least $k-1$ other users. Among the LPPMs that enforce k-anonymity, CliqueCloak [27] use a trusted third party to compute cloaking areas, PRIVE [28] has the same principle but relies on peer-to-peer communication between users to compute the cloaking areas. These two LPPMs allow the protection of a given geo-located point (i.e., online scenario) but do not consider a mobility trace as a whole. Instead, Wait 4 Me (W4M) [19] allows to enforce k-anonimity on mobility traces by extending k-anonymity to (k, δ)-anonymity. In this context, a user mobility trace will be hidden within $k-1$ traces inside a cylindrical volume of radius δ. Figure 2e shows the application of W4M on the two mobility traces of Figure 2d. From these two figures, we observe that the two traces have been distorted to fit into the same cylindrical zone.
Differential privacy [21], which has initially been proposed for database systems, ensures that the result of an agregate query over a table should not be significantly affected by the presence or absence of one single element of this table. This concept has been adapted to mobility data in an LPPM called Geo-Indistinguishability (Geo-I) [14]. In Geo-I, differential privacy is ensured by adding spatial noise to location data generated using a two dimensional Laplacian distribution. An example of applying Geo-I to a mobility trace of Figure 2a is depicted in Figure 2b. In this figure, we observe that each point in the original trace has been translated due to the added noise. As such, it is more difficult to infer information such as user POIs.
In addition to the above LPPMs, there exist other LPPMs that try to protect user mobility traces by removing significant information from the traces such as user POIs. Among these LPPMs, Promesse [22] reaches this objective by distorting the temporal dimension of the mobility trace. Specifically, Promesse erases user POIs by using a speed smoothing technique, which assures that between each successive points in the obfuscated trace the distance and time difference are the same. An example of applying Promesse to a mobility trace of Figure 2a is depicted in Figure 2c. In this figure, we observe that POIs have been removed yet it is still possible to reason about user trajectories.

While the above LPPMs offer various theoretical or practical guarantees to protect the privacy of the users, it is difficult for a system designer to compare them and to know which one will be effective to obfuscate her dataset. For instance, how to assess whether enforcing k-anonymity with the W4M protocol will better protect users than enforcing differential privacy with the Geo-I protocol ?
In this paper, we propose a practical toolkit for helping system designers in the difficult task of obfuscating a dataset. Our toolkit is based on user re-identification attacks as further described in the following section.

3 Modelling re-identification attacks in SFERA

User re-identification attacks are an effective way for assessing LPPMs in practice as they allow to assess whether obfuscated data can be linked back to user former mobility data. We present in this section a generic model for re-identification attacks (Section 3.1) and show how our model can be instantiated to model state-of-the-art re-identification attacks (Section 3.2).

3.1 SFERA-Model: A Generic Model for Re-Identification Attacks

Let $U = \{U_1, U_2, \ldots, U_N\}$ be the set of users in the system. The first phase of a re-identification attack is the training phase in which the adversary builds a knowledge base about the users in the system. In real systems, this phase may correspond to a period of time where users were using a geo-located service without protecting their mobility data. This phase is depicted in the left part of Figure 3. Specifically, we assume that for each user U_i, the adversary has access to a set of mobility traces corresponding to her past mobility, i.e., KD_i (where KD stands for Known user Data). Specifically, the set of all mobility traces known by the adversary is noted $KD = \{KD_1, KD_2, \ldots, KD_k\}$. From each of these traces KD_i, we assume that the adversary builds a user profile $p(KD_i)$ that characterizes the user mobility as depicted in the bottom left part of Figure 3 (Step (1)). This profile is specific to each re-identification attack as further discussed in Section 3.2.

The second phase of a re-identification attack is the re-identification phase. This phase is depicted in the right part of Figure 3. In this phase, we assume that the adversary obtained a set of anonymous mobility traces (Step (2) in the figure), i.e., $UD = \{UD_1, UD_2, \ldots, UD_m\}$ (where UD stands for Unknown user Data). Then, from each anonymous trace UD_i, the adversary builds a profile $p(UD_i)$ containing important information in this trace (Step (3) in the figure). Finally, a re-identification attack **A** run by the adversary tries to re-associate each extracted profile $p(UD_i)$ with profiles of known users, i.e.,

$$\begin{array}{rcccc} A & : & UD & \rightarrow & U \\ & & UD_i & \mapsto & A(UD_i, KD) = U_a \end{array}$$

A key element for the success of a re-identification attack is the similarity metric used to compare anonymous data with known user profiles (Step (4) in Figure 3). In addition to the way user profiles are modelled, the similarity metric is the second element, which is specific to each re-identification attack as further discussed in Section 3.2.

If many anonymous traces are given as input to a re-identification attack, the attack is re-iterated on each element of UD_i as depicted in Algorithm 1. The success of an attack is then computed based on the number of correct re-associations the attack performs between anonymous traces and known user profiles. To do this, we employ an oracle Id able to disclose for each anonymous trace UD_i its owner identity $Id(UD_i) = u(UD_i)$. This way, we can compute

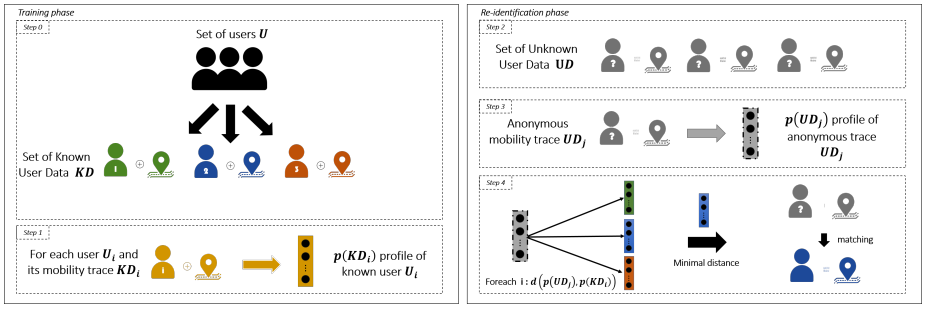


Figure 3: Re-identification attacks process from collecting phase to re-identification phase

the **user re-identification rate** :

$$r(A_k, KD, UD) = \frac{\sum_{UD_i} \begin{cases} 1 & \text{If } A_k(UD_i, KD) = Id(UD_i) \\ 0 & \text{Else} \end{cases}}{|UD|}$$

Algorithm 1 Re-identification attack

function $A(UD, KD)$
  $UP \leftarrow \{p(UD_i) \backslash \forall i\}$
  $KP \leftarrow \{p(KD_j) \backslash \forall j\}$
  $matches \leftarrow \emptyset$
  for $i \leftarrow [\![1, |UD|]\!]$ **do**
    $j \leftarrow \arg \min_{0<j\leq|KD|} d(UP_i, KP_j)$
    $matches \leftarrow matches \cup (Id(UD_i), Id(KD_j))$
  end for
  $rate \leftarrow \dfrac{\sum_{(u',u)\in matches} \begin{cases} 1 & \text{if } u' = u \\ 0 & \text{else} \end{cases}}{|UD|}$
  return $(rate, matches)$
end function

3.2 Existing attacks in the SFERA-Model

In this section we show how two representative re-identification attacks of the literature can be integrated in SFERA. These two attacks are POI-Attack [23], which models user mobility traces as a list of POIs and PIT-Attack [24], which models user mobility traces as Markov chains as further described below.

3.2.1 Points Of Interest Attack - POI-Attack

This attack uses Points of interest (POIs) to characterize users' profiles. Therefore $poi(KD_i)$ is the set of POIs extracted from the trace KD_i. Those points are extracted using clustering algorithms such as the ones presented in [25, 26] parameterized with the diameter of a geographical zone where a user has stopped and a minimum duration characterizing her stop. To measure the similarity between two sets of POIs, each POI of the first set is associated with the geographically closest POIs in the second set. The similarity between the two sets will be equal to one minus the median of all the geographical distances, which is computed as follows :

$$d(X,Y) = median\left[\{\min_t\left[d_{geo}(X_r,Y_t)\right]\setminus\forall r\} \bigcup \{\min_r\left[d_{geo}(X_r,Y_t)\right]\setminus\forall t\}\right]$$

3.2.2 Probabilistic Inter-POI Transition Attack - PIT-Attack [24]

In addition to extracting POIs, this attack takes into consideration the transition probability from one POI to another. Specifically, the authors rely on mobility Markov chains [10] where the states are POIs ($P = P_1, P_2, \ldots, P_k$) ordered by the number points in each POI and the edges' labels are transitions probabilities between POIs (t_{P_i,P_j}). This is done by computing the proportion of transition between each POI in the mobility traces. In order to compute the distance between two mobility Markov chains, two informations are taken into account : the geographical distance between POIs and the weight of each POI. The weight of a POI is computed using the proportion of points contained inside the POI. More precisely the authors proposed many distance metrics to compare Markov chains. The most effective one is the *stats-prox* distance which is a combination of two distances: the stationary distance and the proximity distance. More precisely :

$$d_{stats-prox} \equiv if(d_{stat} > \delta)\ d_{stat}\ else\ d_{prox}$$

with the stationary distance (d_0 is a parameter)

$$d_{stats}(P,Q) = \sum_{P_i,Q_i \in P\times Q} w(P_i) \times \begin{cases} d(P_i,Q_j) & \text{If } d(P_i,Q_j) < d_0 \\ 0 & \text{Else} \end{cases}$$

And the proximity distance (r_0 is a parameter and $r_i = \frac{1}{2}r_{i-1}$)

$$d_{prox}(P,Q) = \left(\sum_{i=1}^{min(|P|,|Q|)} \begin{cases} r_i & \text{If } d(P_i,Q_i) < \Delta \\ 0 & \text{Else} \end{cases}\right)^{-1}$$

This attacks rely almost excursively on POIs, eliminating the information contained inside the trajectories. Also LPPMs focusing on the elimination of POIs

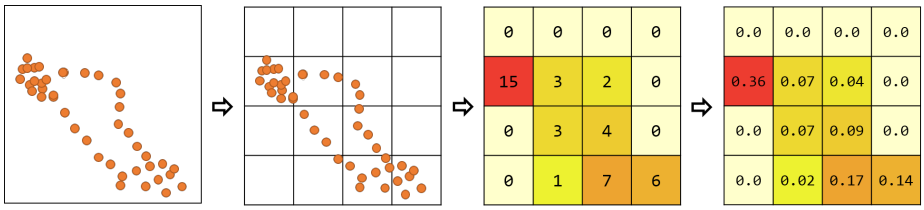


Figure 4: From mobility trace to user profile in AP-Attack

yield to a inept attack as illustrated in Section 6.6. In the next section, we present a novel attack that uses the whole mobility in the construction of the user profile.

4 AP-Attack: A novel attack in the SFERA-Model

We present in this section **AP-Attack** (All Points Attack) a novel re-identification attack that uses the whole user mobility data to form user profiles. Specifically, instead of focusing on a sub-set of points (e.g., those constituting POIs), AP-Attack aggregates all the points enclosed in a user mobility trace into a heat-map structure. More precisely, as shown in Figure 4, the map is subdivided into a grid with cells of the same size. Then, in each cell the number of records found in it is computed. As such, each cell will reflect the intensity of user movement in the corresponding geographical zone. This allows distinguishing between extremely, moderately, slightly frequented cells and unfrequented cells. Thereby, $p_a(KD_i)$ return a probability distribution where each value $p_a(KD_i)^{(k)}$ represents the probability that the owner of the trace U_i goes through the cell k.

Therefore, we can translate the distance between two profiles with the distance between two probability distributions. To compute this distance we can rely on classical distance metrics between probability distributions such as the ones surveyed in [29]. With respect to the experiments we did in Section 6.1.1, one of the best metric to choose from is the Topsoe divergence defined as follows:

$$d_{Topsoe}(P,Q) = \sum_i \left[P_i \ln\left(\frac{2P_i}{P_i+Q_i}\right) + Q_i \ln\left(\frac{2Q_i}{P_i+Q_i}\right) \right]$$

In order to re-identify an anonymous trace UD_i, we match the trace with U_j one of the user of U whose trace KD_j minimize $d(p_a(UD_i), p_a(KD_j))$.
ie : $A(UD_i, KD) = \arg\min_{KD_j \in KD} \left(d(p_a(UD_i), p_a(KD_j))\right)$

This new attack can help assess the effectiveness of an obfuscation technique. This why, this attack is integrated in the toolkit SFERA that we present in the next section as well as how to use it in order to assess LPPMs.

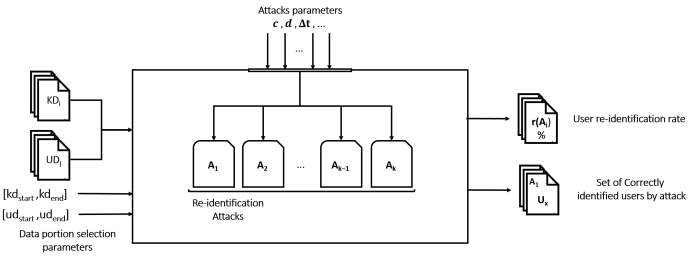


Figure 5: Architecture of SFERA

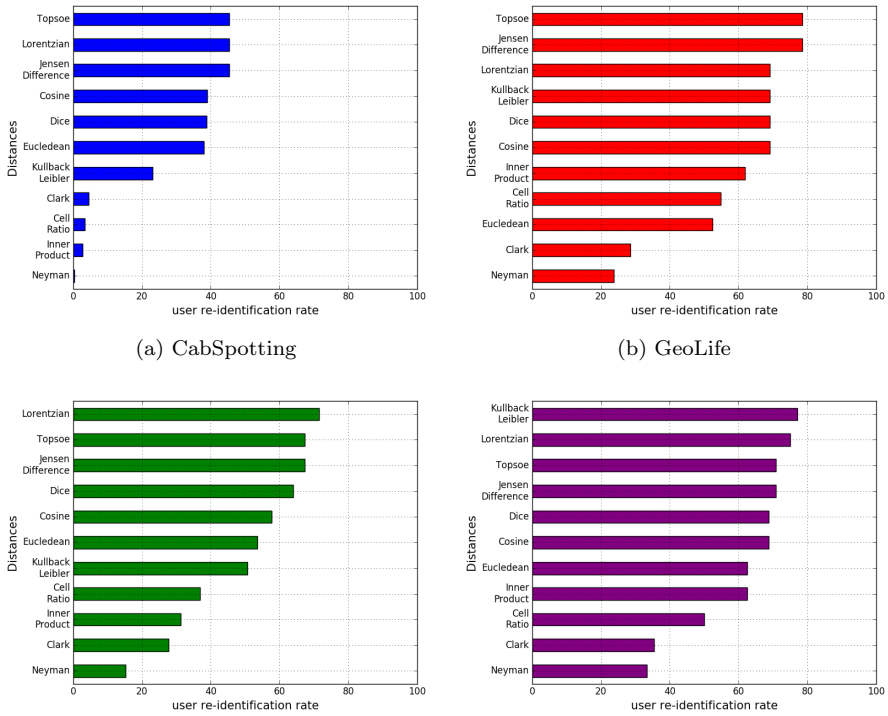
5 Assessing LPPMs using SFERA

We present in this section the SFERA toolkit a practical tool for assessing the effectiveness of LPPMs using re-identification attacks. The code and an executable of the SFERA toolkit can be found online [30]. The current version of the SFERA toolkit contains an implementation of the three attacks described in this paper, i.e., AP-Attack, POI-Attack and PIT-Attack.

As shown in Figure 5, SFERA takes as input two knowledge bases: a set of raw mobility traces (KD) and the same set of traces that have been obfuscated with a given LPPM (UD). In addition, to these two datasets, SFERA takes a configuration file containing the following information: (1) the proportion of traces from KD that should be used as a training set, (2) the proportion of traces from UD that should be used as a testing set and (3) the parameters of the attacks lunched. Then, SFERA produces for each attack implemented in the toolkit the following two outputs: (1) a re-identification rate showing the percentage of obfuscated traces that have been successfully associated to the right user profile and (2) the list of users for which the obfuscation was unsuccessful (i.e., the attacks was able to re-associate the anonymous trace to the right user profile). We show in the following section that using SFERA can help realizing two essential tasks: (1) the comparison of a set of LPPMs and (2) the obfuscation of a given dataset following a user-centric approach. Indeed, running the toolkit with various LPPMs allows on the one hand the comparison of the individual ability of LPPMs to protect users privacy against an adversary that would run one or multiple re-identification attacks. On the other hand, the user based output of SFERA allows a dataset owner to know which LPPM was effective in protecting which user. As such, an obfuscated dataset combining various LPPMs on a per user basis could be produced. These two usecases are further discussed in the following section.

6 Evaluation

We present in this section the evaluation of our proposed SFERA toolkit and show how it can be used to help system designers or data owners to evaluate their LPPM or to obfuscate their dataset (respectively). We start by present-



(a) CabSpotting

(b) GeoLife

(c) MDC

(d) PrivaMov

Figure 6: Comparison distance metrics used in AP-Attack

ing the attacks and LPPMs used in this evaluation and how they have been configured (Section 6.2); our used datasets (Section 6.3) and our experimental setup (Section 6.4). Then, we present the performance of our proposed AP-Attack compared to state-of-the-art attacks (Section 6.5). Finally, we focus on two usecases illustrating how our SFERA toolkit can be used. The first use-case is the study of existing LPPMs when confronted to the attacks included in SFERA (Section 6.6). The second usecase is the use of SFERA for improving data obfuscation through a user-centric multi-LPPM approach (Section 6.7).

6.1 AP-Attack parameters calibration

6.1.1 Distance metric

In the Figure 6, we present different distance metrics used to compare between user profile in AP-Attack. We notice that Topsoe distance and Lorentzian distance are the two best metrics. Topsie being the best distance for two out of four dataset, that's why, we've chosen the Topsoe distance as the distance.

6.1.2 Cell Size

In the Figure 7, we present how the cell size affects the user re-identification rate. We notice that it is dataset-dependent.

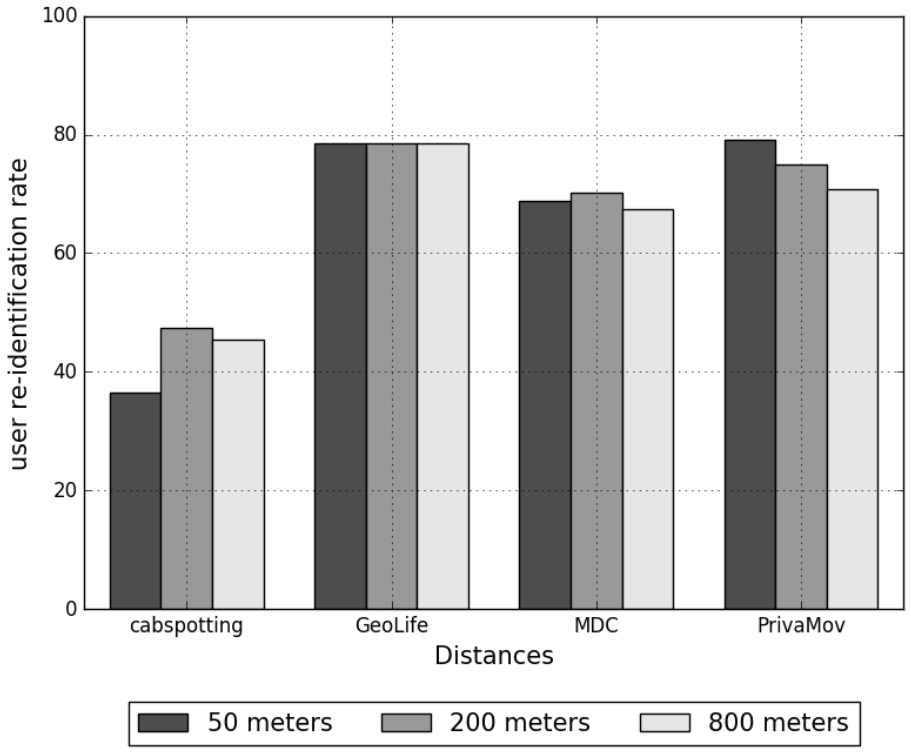


Figure 7: Evaluation of cell Size effect on AP-Attack

6.2 Attacks and LPPMs

The three attacks presented in this paper are included in the SFERA toolkit, i.e, AP-Attack, POI-Attack and PIT-Attack. Each of these attacks has a number of configuration parameters. Specifically, AP-Attack has a cell size parameter that we have fixed at 800 meters in this evaluation. After a number of calibration experiments, we have chosen this value because it was big enough to include POIs and was resilient to noisy traces. Furthermore, POI-Attack and PIT-Attack require parameters for the extraction of the POIs from the traces. These parameters are the diameter of clustering area (that we fixed at 200m) and the minimum time spent inside a POI (that we fixed at 1 hour). These values have been chosen after a series of experimentations.

To assess privacy level obtained by LPPMs, we have selected three different

mechanisms (see section 2.2): (1) Geo-I, which adds Laplacian noise to mobility traces and enforces differential privacy; (2) Promesse, which uses speed smoothing to erase POIs and (3) W4M, which alters traces to group them in cylindrical volumes hence enforcing k-anonymity. Each LPPM has a number of configuration parameters. These parameters have an impact on the privacy level offered to the users but also on the quality of the resulting obfuscated data. Due to a lack of space, we decided to configure each LPPM following a medium level of protection. This choice is motivated by the fact that our objective is not to find the best LPPM in the literature but rather to show how our toolkit can be used to compare LPPMs and to help obfuscating data. Other experiments with other configurations of the used LPPMs or using other LPPMs of the literature can be done using our available toolkit [30]. Specifically, Geo-I is configured with a parameter ϵ that has an impact on the amount of noise added to the data (the lower epsilon the higher the noise). We have fixed the value of this parameter to 0.01, which corresponds to medium privacy level. Promesse is configured with a parameter α that corresponds to the distance between two successive sampling points. We have fixed this parameter at 200 meters. Finally, W4M is configured with two parameters, k representing the minimum number of users inside the cylindrical volume and the radius δ of the latter. We have fixed these parameters at $k = 2$ and $\delta = 600$ meters because W4M erases a lot of points making the dataset almost empty and those parameters guarantee privacy and availability of the data.

6.3 Datasets

We used four real mobility datasets in our experiments. These datasets are:(1) Cabspotting [31] that contains the mobility of 536 cab drivers in the city of San Francisco; (2) Geolife [32] that contains the mobility of 42 users mainly in the city of Beijing; (3) MDC [4] that contains the mobility data of 144 users in the city of Geneva and (4) PrivaMov [33] that contains the mobility of 48 students and staff members in the city of Lyon. To make the comparison fair between the datasets, we selected in each dataset the 30 most active successive days. We present in the table 1 a description of the datasets used in our experiments. In all the experiments described in this paper, we split the datasets into a period of 15 days used for the training phase and 15 days used for the re-identification phase. We run other experiments where the training and re-identification phases were varied from 1 day to 23 days each to evaluate the impact of dataset splitting on re-identification attacks. We do not present these results in the paper due the lack of space, but the results are available in the companion technical report [30].

6.4 Experimental setup

All of our experiment were carried out in a computer running an Ubuntu 14.04 OS with 50GB of RAM and 16 cores of 1.2Ghz each. The prototype of SFERA was written in Java & Scala and runs in the Java Virtual Machine 1.8.0.

Table 1: Description of datasets

Name	CabSpotting	Geolife	MDC	PrivaMov
# users	536	42	144	48
Localization	San Francisco	Beijing	Geneva	Lyon
# records	11.219.955	1.574.338	904.422	973.684

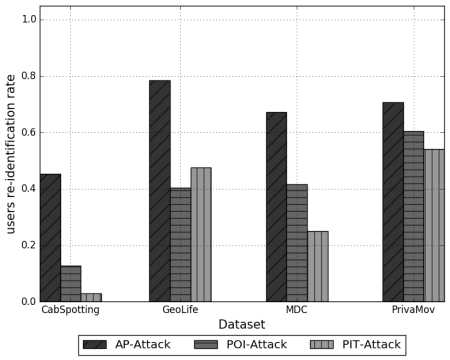
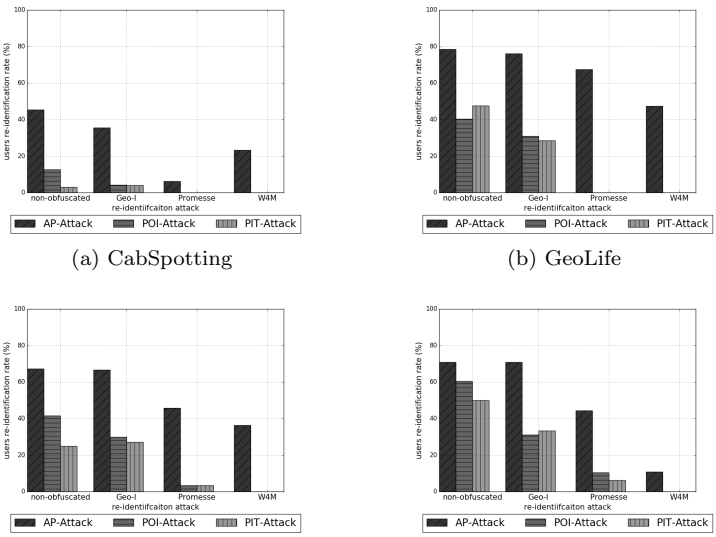


Figure 8: Performance of re-identification attacks

6.5 Performance of re-identification attacks

The first experiment we did was intended to compare the three considered re-identification attacks by measuring their re-identification rate on non-obfuscated data of the four considered datasets. Results are depicted in Figure 8. From this figure, we observe that AP-Attack outperforms the two other attacks on all the considered datasets. This experiment shows that sending mobility data "anonymously" (e.g., by using anonymous communication protocols such as TOR [34]) to application providers is not sufficient to protect the privacy of users as adversary using re-identification attacks is able to de-anonymise from 45% to 80% of the traces in the four datasets. It is thus necessary for end users to rely LPPMs to protect their data. From this experiment we also notice that Cabspotting is the dataset where the users are the most intrinsically protected. This comes from the fact that taxi drivers have similar mobility patterns (e.g., they regularly go to the airport, famous hotels, malls and the taxi parking places). Instead, MDC, GeoLife and PrivaMov are related to users having different mobility habits, which makes them easier to de-anonymize.



(a) CabSpotting (b) GeoLife

(c) MDC (d) PrivaMov

Figure 9: Performance of LPPMs

6.6 Usecase1: Assessing the Performance of LPPMs using SFERA

In this experiment, we compare the performance of the three considered LPPMs, i.e., Geo-I, Promesse and W4M. Specifically, we evaluate the re-identification rate obtained by the three former attacks data obfuscated using these three LPPMs. Figure 9 shows the result of this experiment. In addition to the three LPPMs, we report the results obtained for non-obfuscated data, which we use as a baseline. At first glance, we observe the high level of privacy enforced by W4M in the PrivaMov dataset (11%) and by Promesse in the Cabspotting dataset (6%) against AP-Attack, which is the most successful attack. Nevertheless, these two LPPMs seem not to be sufficient to protect users in the GeoLife and MDC datasets where the re-identification rate reaches 48% and 36% for W4M and 68% and 46% for Promesse. Finally, we observe that Geo-I is the least efficient LPPM against re-identification attack in the four datasets. Summarizing, this experiment allows us to draw the following conclusions: (1) there is no one-size-fits-all LPPM, as the resilience of an LPPM to re-identification attacks depends on the underlying data; (2) users of a given dataset are not all equal in front of re-identification attacks, as on the four datasets there exist users that are never re-identified even in the absence of protection mechanisms (e.g., 54% for the best case with Cabspotting and 21% for the worst case with Geolife). These two observations motivate the need of investigating multi-LPPM and user centric data obfuscation techniques as presented in the following section.

6.7 Usecase2: Improving Dataset Obfuscation using SFERA

This usecase aims at showing how our SFERA toolkit can help a data owner improving the obfuscation of her dataset. We start this experiment by evaluating the sensitivity of individual users to re-identification attacks (Section 6.7.1). We then investigate a multi-LPPM protection scheme (Section 6.7.2).

6.7.1 Sensitivity of users to re-identification attacks

This experiment shows the proportion of users protected by none, one or multiple LPPMs on each of our four datasets. In this experiment we used all the re-identification attacks of our toolkit. Results are depicted in Figure 10. Overall these results allow us draw the following conclusions: (1) there is a proportion of users are not vulnerable to re-identification attacks (this proportion varies from 19% to 54% in the four datasets); (2) there is a proportion of users that can not be protected by the existing LPPMs in their current configuration (this proportion varies from 2% to 33% in the four datasets); (3) there is a proportion of users that can be protected by only one LPPM among those that we tested (this proportion varies from 19% to 42% in the four datasets) and (4) there is a proportion of users that can be protected by multiple LPPMs (this proportion varies from 12% to 37% in the four datasets). From these conclusion, which to the best of our knowledge we are the first to draw, it becomes natural to think of multi-LPPM obfuscation techniques as further discussed in the following section.

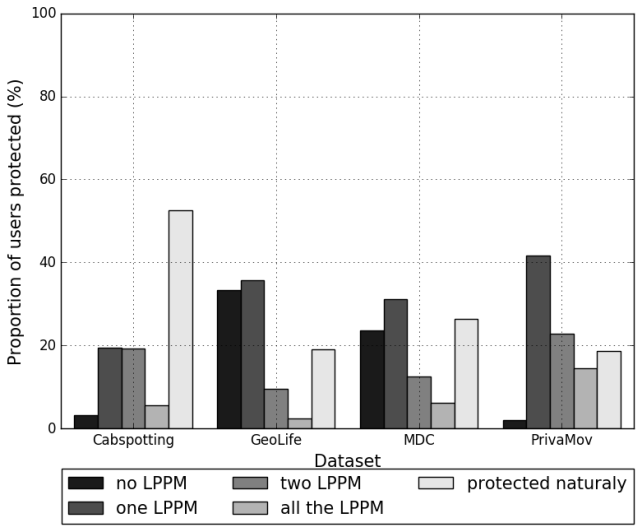


Figure 10: Proportion of users protected by a number of LPPM

6.7.2 Towards Multi-LPPM Obfuscation

In this experiment, we decided to leverage the results obtained in the previous experiment to design a multi-LPPM obfuscation technique. Specifically, on each of our four datasets we built an obfuscated dataset as follows. First, we took all the users that were insensitive to all the re-identification attacks. As these users are naturally protected, it is better not to alter their corresponding portion of the data in the corresponding datasets. Then, for all the users that were protected by only one LPPM, we used the latter in our obfuscated dataset. Finally, for those users that were protected by more than one LPPM, we used in the following order Geo-I, Promesse or W4M to obfuscate their data. This choice was motivated by the degree of degradation obtained in the traces after obfuscation, which is lower when using Geo-I and Promesse than when using W4M.

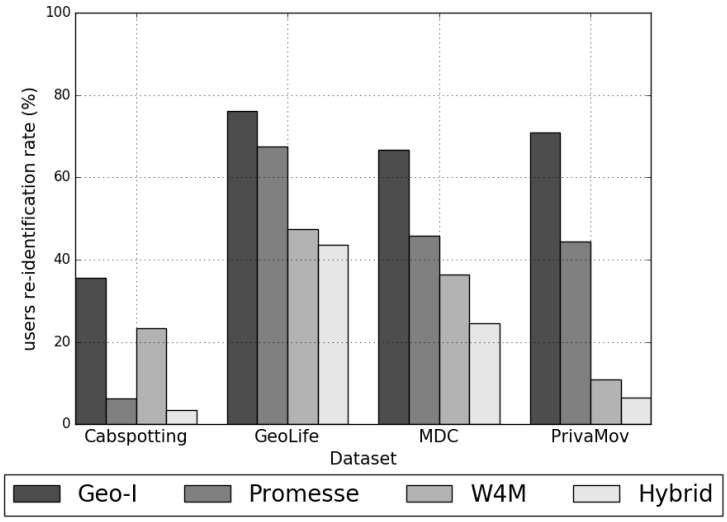
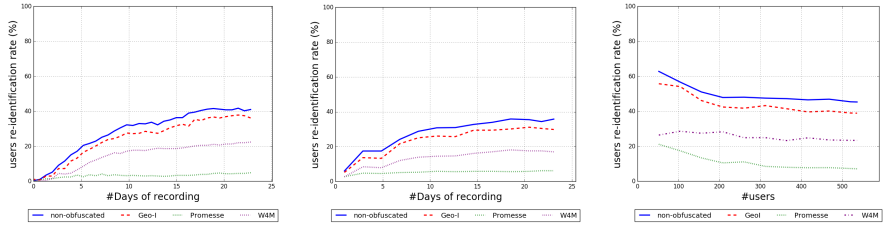


Figure 11: Performance of the Hybrid LPPM

The results depicted in Figure 11 show that our multi-LPPM and user-centric obfuscation technique called Hybrid in the figure outperforms all the existing LPPMs. Nevertheless, there are still users that are not protected by our multi-LPPM approach. This suggests that there is still room for proposing novel LPPMs. Our findings suggest that efforts should go in the direction of a data-centric/user-centric approach. We showed in this section how SFERA could help a system designer or data owner going towards this direction by adapting the LPPMs and possibly their degree of protection according to the sensitivity of each user to re-identification attacks.



(a) variation in Known data - 1day to 23days

(b) variation in Unknown data - 1day to 23days

(c) variation in # users of system

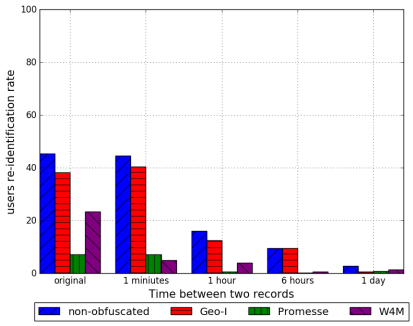
Figure 12: Quantity of data effects on re-identification on the cabspotting dataset

6.8 Quantity of data effects on re-identification attack and LPPMs

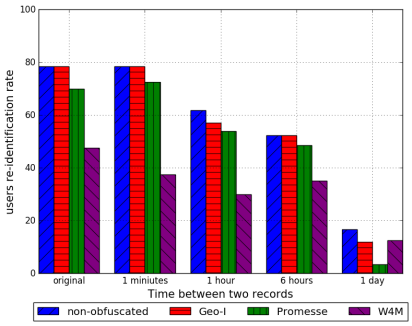
In this experiment, we want to highlight the impact of quantity of data available for the re-identification. in the figure 12a, we show, the evolution in data available in the known data to form the user profiles of known user. The Cabspotting dataset is constituted of 30days of recording, we leave out 7days for the anonymous traces to be re-identified. We notice that the 20% rate is obtained with only 5days of recording in the non-obfuscated data. rate obtained with 15 days with W4M. We notice also that the increase in the number of days in the known data increase the rate. In the figure 12b, we leave out 7days of recording to form known users profiles. We then vary the number of days of recording in the anonymous mobility trace. We notice a similar trend than in the variation of number of days in recording in known data, except that the rates are smaller. This shows the importance of constructing complete user profiles in the known data, because they will highlight the dissimilarities between users' behaviors. While, anonymous traces' profiles won't be compared to each other.
In the figure 12c, we show how the number of users in the system affects the re-identification rate. To do that, we select randomly k users of the dataset then cut the dataset into two halves and lunch the AP-Attack (we iterate 3 times because of the randomization). The Cabspotting dataset from all the datasets is the most accurate to show the effect of such variation because it possesses the biggest number of users 536. Surprisingly, the re-identification rate decrease form 50 users until 200 users but stagnates between 200 and 536 users. This should be further investigated by constructing dataset with more users which is not available at the time.

7 Related work

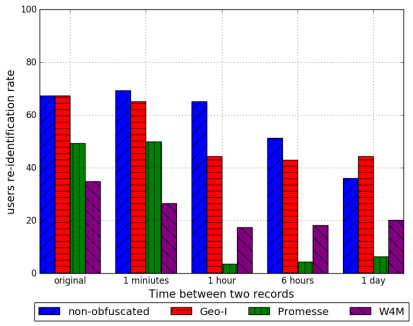
The re-identification threat is affecting a wide variety of systems due to the wide scale gathering of user personal data by application providers. To mea-



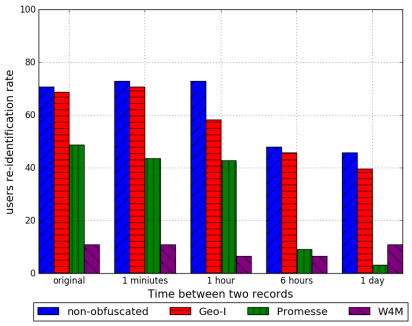
(a) Cabspotting



(b) Geolife



(c) MDC



(d) PrivaMov

Figure 13: Sampling effects on re-identification attack

sure this threat, a variety of re-identification attacks are being proposed in various systems such as Web-search systems [35, 36], face recognition [37], social networks [38] and recommender systems [39]. User re-identification attacks in the context of mobility data such as the one proposed in this paper, share a similar objective as the attacks above. Specifically, re-identification attacks demonstrate that the accumulation of mobility data about users allows the extraction of user profiles despite users hiding or changing their user ID. In order to protect against these threats various Location Privacy Protection Mechanism (LPPM) have been introduced. As previously discussed in this paper, LPPMs alter mobility traces in order to protect users against the inference of sensitive information about them. To evaluate the degree of protection offered by LPPMs to users, various privacy evaluation metrics have been used. Examples of such metrics include the POI retrieval rate [40, 22], which reflects the a ability of a LPPM to hide user POIs in the obfuscated traces.

Closer to our work, there have been two frameworks for evaluating LPPMs. The first one by Shokri & al. [40] includes a set of statistical attacks and the consider three dimensions for evaluation of LPPMS: the *certainty* of the adversary with his result, the *accuracy* of the attack results and the *correctness*, which is the distance between the attack results with and without protection. However, this framework only works with probabilistic LPPMs performing basic operations (e.g., adding noise, adding dummy regions, merging regions, suppressing locations). The second framework is the GEPETO toolkit [10]. This toolkit includes the re-identification attack based on Markov chains that we integrated in SFERA.

8 Conclusion

In this paper, we presented SFERA, a toolkit to assess the effectiveness of location privacy protection mechanisms (LPPMs) in practice using re-identification attacks. SFERA includes three re-identification attacks, two of which are state-of-the-art attacks in addition to AP-Attack, a novel re-identification attack based on a heat-map representation of user profiles. We showed that this attack, which aggregates user mobility into a probability distribution acting as a fingerprint of user mobility, outperforms existing attacks on four real mobility datasets. Moreover, two uses cases of SFERA were presented and analysed. The first use case, which aimed at comparing the ability of three state-of-the-art LPPMs to protect users against re-identification attacks showed that there is no one-size-fits-all LPPM. Instead, the degree of protection offered by LPPMs heavily depend on the underlying data. We then decided to further analyse in a second use case how individual users are sensitive to re-identification attacks while being protected by various LPPMs. Our results have shown that users are not equal in front of re-identification attacks, some can not be protected by the considered LPPMs, some are naturally protected against, while others can be protected by one or multiple LPPMs. This observation, that to the best of our knowledge we are the first to establish has lead us to the design of a Multi-

LPPM user-centric obfuscation technique, which better resists re-identification attacks. Still, according to the considered dataset, we showed that a proportion of users can not be protected using this technique, which opens the door for future investigations in the field. In this context, we have shown that the SFERA toolkit can be key to help system designers in the testing and tuning of novel LPPMs and to help data owners in user-centric obfuscation of her dataset.

References

[1] Google, "Google maps." [Online]. Available: https://maps.google.com

[2] Foursquare-Labs, "Swarm." [Online]. Available: https://www.swarmapp.com

[3] Niantic, "Pokemon Go." [Online]. Available: http://www.pokemongo.com

[4] J. K. Laurila, D. Gatica-Perez, I. Aad, B. J., O. Bornet, T.-M.-T. Do, O. Dousse, J. Eberle, and M. Miettinen, "The Mobile Data Challenge: Big Data for Mobile Computing Research," in *Pervasive Computing*, 2012.

[5] "Open data in USA." [Online]. Available: https://www.data.gov/

[6] "Open data in UK." [Online]. Available: https://data.gov.uk/

[7] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[8] M. Terrovitis, "Privacy Preservation in the Dissemination of Location Data," *SIGKDD Explor. Newsl.*, vol. 13, no. 1, pp. 6–18, 2011.

[9] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 163–175, 2014.

[10] S. Gambs, M.-O. Killijian, and M. Nez Del Prado Cortez, "Show Me How You Move and I Will Tell You Who You Are," *Transactions on Data Privacy*, vol. 4, pp. 103–126, 2011.

[11] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *International Conference on Pervasive Computing*. Springer, 2009, pp. 390–397.

[12] L. Franceschi-Bicchierai, "Redditor cracks anonymous data trove to pinpoint muslim cab drivers." 2015.

[13] I. Bilogrevic, K. Huguenin, M. Jadliwala, F. Lopez, J.-P. Hubaux, P. Ginzboorg, and V. Niemi, "Inferring Social Ties in Academic Networks Using Short-Range Wireless Communications," *Wpes*, pp. 179–188, 2013.

[14] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-Indistinguishability: Differential Privacy for Location-Based Systems," *Ccs'13*, vol. abs/1212.1, pp. –, 2013.

[15] K. Micinski, P. Phelps, and J. S. Foster, "An Empirical Study of Location Truncation on Android," *Most'13*, 2013.

[16] B. Henne, C. Kater, M. Smith, and M. Brenner, "Selective cloaking: Need-to-know for location-based apps," pp. 19–26, 2013.

[17] M. Gramaglia and M. Fiore, "Hiding Mobile Traffic Fingerprints with GLOVE," in *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '15. New York, NY, USA: ACM, 2015, pp. 26:1—-26:13.

[18] O. Abul, F. Bonchi, and M. Nanni, "Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases," in *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*, ser. ICDE '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 376–385.

[19] O. Abul, F. Bonchi, and M. Nanni, "Anonymization of moving objects databases by clustering and perturbation," *Information Systems*, vol. 35, no. 8, pp. 884–910, 2010.

[20] P. Samarati and L. Sweeney, "Generalizing Data to Provide Anonymity when Disclosing Information," in *Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, ser. PODS '98. New York, NY, USA: ACM, 1998, pp. 188—-.

[21] C. Dwork, *Differential Privacy: A Survey of Results*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–19.

[22] V. Primault, S. Ben Mokhtar, C. Lauradoux, and L. Brunie, "Time distortion anonymization for the publication of mobility data with high utility," *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 539–546, 2015.

[23] V. Primault, S. Ben Mokhtar, C. Lauradoux, and L. Brunie, "Differentially Private Location Privacy in Practice," *Most'14*, no. October, 2014.

[24] S. Gambs, M.-O. Killijian, and M. N. d. P. Cortez, "De-anonymization Attack on Geolocated Data," *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 789–797, 2013.

[25] C. Zhou, D. Frankowski, P. Ludford, S. Shekhar, and L. Terveen, "Discovering Personal Gazetteers: An Interactive Clustering Approach," in *Proceedings of the 12th Annual ACM International Workshop on Geographic Information Systems*, ser. GIS '04. New York, NY, USA: ACM, 2004, pp. 266–273.

[26] R. Hariharan and K. Toyama, "Project Lachesis: Parsing and Modeling Location Histories," in *Geographic Information Science: Third International Conference, GIScience 2004, Adelphi, MD, USA, October 20-23, 2004. Proceedings*, M. J. Egenhofer, C. Freksa, and H. J. Miller, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 106–124.

[27] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, ser. ICDCS '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 620–629.

[28] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems," in *Proceedings of the 16th International Conference on World Wide Web*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 371–380.

[29] S.-h. Cha, "Comprehensive Survey on Distance / Similarity Measures between Probability Density Functions," *International Journal of Mathematical Models and Methods in Applied Sciences*, vol. 1, no. 4, pp. 300–307, 2007.

[30] "SFERA and its technical report." [Online]. Available: https://github.com/mmaouche-insa/SFERA/

[31] M. Piorkowski, N. Sarafijanovic-djukic, and M. Grossglauser, "CRAWDAD data set epfl/mobility (v. 2009-02-24)."

[32] Y. Zheng, X. Xie, and W.-Y. Ma, "GeoLife: A Collaborative Social Networking Service among User, location and trajectory," *IEEE Data(base) Engineering Bulletin*, 2010.

[33] A. Boutet, S. B. Mokhtar, and V. Primault, "Uniqueness Assessment of Human Mobility on Multi-Sensor Datasets," 2016.

[34] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," San Diego, CA, 2004.

[35] A. Gervais, R. Shokri, A. Singla, S. Capkun, and V. Lenders, "Quantifying Web-Search Privacy," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 966–977, 2014.

[36] A. Petit, T. Cerqueus, A. Boutet, S. B. Mokhtar, D. Coquil, L. Brunie, and H. Kosch, "SimAttack: private web search under fire," *Journal of Internet Services and Applications*, vol. 7, no. 1, p. 2, 2016.

[37] M. Farenzena, L. Bazzani, A. Perina, V. Murino, and M. Cristani, "Person re-identification by symmetry-driven accumulation of local features," pp. 2360–2367, 2010.

[38] A. Narayanan, E. Shi, and B. I. P. Rubinstein, "Link prediction by de-anonymization: How We Won the Kaggle Social Network Challenge," pp. 1825–1834, 2011.

[39] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 111–125, 2008.

[40] R. Shokri, G. Theodorakopoulos, J. Y. Le Boudec, and J. P. Hubaux, "Quantifying location privacy," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 247–262, 2011.