

# 攻撃者のモデル化を用いた軌跡情報の匿名性評価法

正木 彰伍<sup>1</sup>

**概要:** 本稿では、匿名化された軌跡情報から個人が再識別されるリスクについて、攻撃者の背景知識生成法と攻撃手法からなる攻撃者のモデル化を用いた匿名性評価法を提案する。攻撃者の背景知識生成法は、ある時間帯におけるある個人の軌跡情報を取得できるのは1つの事業者に限らないという軌跡情報の性質に基づき、元データから現実的な背景知識を生成するものである。攻撃手法は、匿名化データ中の軌跡と背景知識中の軌跡との距離を計測することにより、個人を強力的に再識別するものである。提案する匿名性評価法を、実際の軌跡情報を匿名化したデータに適用する実験も行う。結果、提案する攻撃者モデルに対して、本稿で用いた実データの匿名性を向上させるためには、ノイズ付加よりもサンプリングの方が有効であることがわかった。このように、本稿で提案する匿名性評価方法を用いることで、現実に存在する攻撃者に対して、再識別リスクを低減するために適切な匿名化手法を選択することが可能になる。

**キーワード:** パーソナルデータ, 軌跡情報, 匿名性評価, 再識別

## Anonymity evaluation of trajectory data with modeling adversary

SHOGO MASAKI<sup>1</sup>

**Abstract:** In this paper, we propose a novel anonymity evaluation method for the re-identification risk of anonymized trajectory data. Our method consists of adversary background knowledge generation and an attack. We generate realistic adversary background knowledge from an original trajectory data based on the fact that more than two service providers can collect an individual's trajectory at a certain time range. The attack is done by measuring distances between anonymized trajectories and ones in adversary background knowledge to re-identify individuals effectively. We also apply our method to a real trajectory dataset. We find that a sampling method is more effective than a noise adding method to reduce the re-identification risk of the real dataset. Thus our proposed method is helpful to find the effective anonymization method for the target dataset.

**Keywords:** personal data, trajectory data, anonymity evaluation, re-identification

### 1. 導入

#### 1.1 背景

昨今の様々な技術発展により、パーソナルデータと総称される個人にまつわる情報が大量に事業者に蓄積されるようになっている。データを分析し、新たな知見を得ることで、学術分野やビジネスにおいても新たな価値が創造されることが期待されるため、パーソナルデータの利活用が注目を集めている。中でも、パーソナルデータをより幅広く

利活用するため、パーソナルデータ保有者が、データ収集時と異なる目的における利活用をする目的外利用や、第三者である事業者がパーソナルデータを受領し、利活用する第三者提供といった二次利用と呼ばれる新たな活用モデルも検討されている。<sup>\*1</sup>

本稿では、パーソナルデータの中でも、時刻・緯度・経度で表される個人の位置情報の時系列データに注目し、これを軌跡情報と呼ぶ。軌跡情報は、GPSを搭載した携帯端

<sup>1</sup> 日本電信電話株式会社 NTT セキュアプラットフォーム研究所  
NTT Secure Platform Laboratories, NTT Corporation

<sup>\*1</sup> 日本においては、2017年5月30日に改正個人情報保護法が施行され、データに含まれる個人を特定できないよう適切に加工し、匿名加工情報とすれば目的外利用や第三者提供といった二次利用が認められるようになっている。

末により容易に取得することができるため、スマートフォンの普及に伴い、事業者は個人の軌跡情報を大量に保有することが可能となっている。軌跡情報の分析により得られる知見は、データ保有者でない小売業者の出店計画立案といったマーケティング用途や政府・自治体の都市計画立案といった公共用途などにおいて有益であることが期待できるため、第三者提供のニーズが強いパーソナルデータの1つであるといえる。

パーソナルデータの二次利用が注目される一方で、データに含まれる個人の様々なプライバシー侵害が懸念され、このリスクを低減するための対策が求められている。技術的な対策として例えば、 $k$ -匿名化 [1], [2] や差分プライバシー [3] といったパーソナルデータを加工することでデータを保護する手法が広く研究されている。軌跡情報に特化した手法を提案した既存研究の例としては、[4], [5], [6], [7], [8], [9], [10] 等がある。

そのようなデータ加工による匿名性向上の効果を評価するためには、背景知識と攻撃手法からなる攻撃者モデルに基づいて、加工データを攻撃し、評価することが有効な手段の1つである。ただし背景知識は、対象とするパーソナルデータの性質を考慮したうえで、現実想定されるものであるべきである。そのうえで十分な匿名性を担保しているか評価するためには、攻撃手法は、現実的な背景知識を最大限利用した強力な手法であるべきである。

## 1.2 目的・動機

本稿は、匿名化されたうえで公開もしくは第三者提供された軌跡情報から個人が再識別されるリスクに対して、攻撃者のモデル化に基づく匿名性評価法を提案することが目的である。再識別リスクに着目した理由は、特定個人に直結するという意味で直接的なプライバシー侵害であることによる。<sup>\*2</sup>

攻撃者が持ちうる背景知識を考える上で重要な軌跡情報の性質として、ある時間帯におけるある個人の軌跡情報を取得できるのは1つの事業者に限らない、ということがある。このことは、スマートフォンで別の事業者が運営する2つ以上の位置情報を利用するアプリケーションを同時に起動することを想像すれば容易に理解できる。加えて、個人の軌跡は唯一になりやすいという性質も持っている。したがって、ある軌跡情報保有者が公開したデータに対して、別の軌跡情報保有者が、自身が持つ軌跡情報と突き合わせることで、容易に再識別を行えるというリスクが考えられる。

軌跡情報の性質に基づいたこの再識別リスクは現実想定されるものと考えられるが、これまで当該リスクに対する匿名性評価の方法は確立されておらず、軌跡情報

の安全な公開もしくは第三者提供を実現するための課題となっている。

## 1.3 本稿の成果

本稿の成果は、攻撃者モデルを用いた上記リスクに対する軌跡情報の匿名性評価の提案である。具体的には以下の2つからなる。

- (1) ある時間帯におけるある個人の軌跡情報を複数事業者が取得可能という軌跡情報の特徴に基づき、元データから攻撃者の現実的な背景知識を生成する方法の提案
- (2) 匿名化された軌跡情報と背景知識中の軌跡情報との距離を測ることにより、匿名化データから個人を再識別する強力な攻撃手法の提案

実際に、公開されている実際の軌跡情報を用いて、2つの手法（ノイズ付加、サンプリング）で匿名化された軌跡情報の匿名性評価も行う。結果、提案する攻撃者モデルに対して、実験に用いたデータセットの匿名性を向上させるには、ノイズ付加よりも位置情報レコードのサンプリングの方が効果的であることがわかった。このように現実的な攻撃者モデルに対して、匿名性向上のためにはどのような匿名化が適切なのか判断できるという点に、本稿で提案する匿名性評価法の重要性がある。

## 1.4 既存研究との比較

軌跡情報から個人を再識別する攻撃については、これまで広く研究されている。[11], [12] は、家と職場の位置情報を用いた場合の再識別について報告している。しかし、軌跡情報の中に家と職場に対応する位置情報レコードが含まれるとは限らない。本稿では、家と職場の位置情報に限らないより一般的な軌跡情報に関する再識別リスクを評価する。また近年、マルコフ連鎖を用いて長期間に渡る軌跡情報を訓練データとして学習し、個人の移動の傾向を反映した遷移行列を算出し、テストデータから個人を再識別する手法が研究されている [13], [14], [15], [16]。しかし、学習に足る十分な軌跡情報を持ち合わせない攻撃者モデルの方がより現実的であると考えられる。本稿は、ある時間間隔において攻撃者が持ち合わせている背景知識と、匿名化され公開された軌跡情報の直接的な突き合わせにより、個人を再識別するリスクを評価する方法を提案する。

以降の本稿の構成は以下のとおりである。2節で、扱う軌跡情報の形式や表記の定義を行ったうえで、3節で本稿の主眼である匿名性評価方法を提案する。4節で実験準備、5節で実験内容と結果を示す。最後に6節で、本稿のまとめを行う。

## 2. 事前準備

本節では、扱う軌跡情報の形式や表記の定義を行う。

<sup>\*2</sup> 特定個人の識別防止は、日本の改正個人情報保護法における匿名加工情報の要件にもなっている。

表 1 本稿で取り扱う，個人 ID，時刻，緯度，経度のみからなる軌跡情報の例．時刻は UNIX 時刻で表記．

個人 ID	時刻	緯度	経度
0	1212616413	37.748910	-122.397570
0	1212616473	37.748610	-122.397480
0	1212616533	37.748660	-122.397490
0	1212616593	37.748720	-122.397520
1	1211063136	37.646790	-122.406600
1	1211516754	37.807650	-122.412320
1	1211780355	37.753060	-122.505730

表 2 本稿における軌跡情報に関する表記．

$D$ の位置情報レコード総数	$ D $
$D'$ の位置情報レコード総数	$ D' $
$A$ の位置情報レコード総数	$ A $
$D$ 中の個人の総数	$N_D$
$D'$ 中の個人の総数	$N_{D'}$
$A$ 中の個人の総数	$N_A$
$D$ 中の $i$ 番目の個人の軌跡情報	$d_i$
$D'$ 中の $i$ 番目の個人の軌跡情報	$d'_i$
$A$ 中の $i$ 番目の個人の軌跡情報	$a_i$
$d_i$ の位置情報レコード総数	$ d_i $
$d'_i$ の位置情報レコード総数	$ d'_i $
$a_i$ の位置情報レコード総数	$ a_i $
$d_i$ の $j$ 番目の { 時刻, 緯度, 経度 }	$d_i(j).{t, \text{lat}, \text{lon}}$
$d'_i$ の $j$ 番目の { 時刻, 緯度, 経度 }	$d'_i(j).{t, \text{lat}, \text{lon}}$
$a_i$ の $j$ 番目の { 時刻, 緯度, 経度 }	$a_i(j).{t, \text{lat}, \text{lon}}$

## 2.1 扱う軌跡情報の形式

本稿では，個人 ID，時刻，緯度，経度のみからなる軌跡情報として最も簡素な形式を扱う．表 1 に例示する．

## 2.2 表記

元データを  $D$ ， $D$  を匿名化したデータを  $D'$ ， $D$  から生成した攻撃者の背景知識を  $A$  とする．その他の表記は，表 2 にまとめる．ただし，各個人の軌跡は時刻で昇順ソートされているとする．つまり， $d_i$  を例に取ると， $d_i(j).t < d_i(j+1).t$  である．

## 3. 提案手法

本節では，本稿が提案する軌跡情報の匿名性評価における二要素である攻撃者の背景知識生成方法と攻撃手法について述べる．

### 3.1 攻撃者の背景知識生成方法

本稿が着目する軌跡情報の性質として，ある時間帯におけるある個人の軌跡情報を取得できるのは 1 つの事業者に限らない，ということがある．ただし，取得する時刻，位置情報の数は事業者によって異なることが一般的であろうと予想される．このことに基いて，元データから攻撃者の現実的な背景知識を生成する．より具体的には，緯度，経度を時刻の一次関数で近似して，線形補間を用いてランダ

ムに生成する．

$D$  に含まれるある個人  $i$  の軌跡情報  $d_i$  から攻撃者の背景知識  $a_i$  における  $k$  番目の位置情報  $a_i(k)$  を得るために，具体的には以下の手順を踏む．

- (1)  $[1, |d_i| - 1]$  の範囲で，一様乱数を発生させ，整数  $j$  を得る．
- (2)  $[d_i(j).t, d_i(j+1).t]$  の範囲で，一様乱数を発生させ，時刻  $a_i(k).t$  とする．
- (3) 以下で定義する  $\alpha_{ij,\text{lat}}$ ， $\beta_{ij,\text{lat}}$ ， $\alpha_{ij,\text{lon}}$ ， $\beta_{ij,\text{lon}}$  を算出する．

$$\alpha_{ij,\text{lat}} = \frac{d_i(j).\text{lat} - d_i(j+1).\text{lat}}{d_i(j).t - d_i(j+1).t} \quad (1)$$

$$\beta_{ij,\text{lat}} = d_i(j).\text{lat} - \alpha_{ij,\text{lat}} \times d_i(j).t \quad (2)$$

$$\alpha_{ij,\text{lon}} = \frac{d_i(j).\text{lon} - d_i(j+1).\text{lon}}{d_i(j).t - d_i(j+1).t} \quad (3)$$

$$\beta_{ij,\text{lon}} = d_i(j).\text{lon} - \alpha_{ij,\text{lon}} \times d_i(j).t \quad (4)$$

- (4) 線形補間により，以下のようにして  $a_i(k)$  を得る．

$$a_i(k).\text{lat} = \alpha_{ij,\text{lat}} \times a_i(k).t + \beta_{ij,\text{lat}} \quad (5)$$

$$a_i(k).\text{lon} = \alpha_{ij,\text{lon}} \times a_i(k).t + \beta_{ij,\text{lon}} \quad (6)$$

以上を  $|a_i|$  回繰り返すことで， $a_i$  を得る． $|a_i|$  はパラメータとして与える．

### 3.2 攻撃手法

背景知識を用いて，匿名化データから個人を再識別する攻撃手法は様々考えられる．これまで行われた PWS Cup では，レコード間距離やレコードソート，レコードの一致に基づく再識別アルゴリズムが採用されてきた [17], [18], [19]．その中でも，レコード間距離に基づき，最小距離となるレコードを再識別するアルゴリズムが強力であったと報告されている [20]．

そこで本稿では，地理的な距離を用いて  $d'_i$  と  $a_j$  の距離を計測し，最小距離となる個人を  $D'$  から探索する攻撃を提案する．まず， $D'$  から  $a_j$  と時間帯に重複のある  $d'_i$  を探索する．しかし，時間帯に重複があっても  $d'_i$  と  $a_j$  が同時刻での位置情報を有しているとは限らないため，軌跡間距離の定義は非自明である．そこで，本稿では再び線形補間を用いて以下のように定義する  $d'_i$  と  $a_j$  の距離  $L(d'_i, a_j)$  を算出する．

- (1)  $d'_i$  の中から， $a_j(n).t$  と最も近い 2 つの時刻  $d'_i(m).t$ ， $d'_i(m+1).t$  を探索する．

- (2) 以下で定義する  $\alpha'_{im,\text{lat}}$ ， $\beta'_{im,\text{lat}}$ ， $\alpha'_{im,\text{lon}}$ ， $\beta'_{im,\text{lon}}$  を得る．

$$\alpha'_{im,\text{lat}} = \frac{d'_i(m).\text{lat} - d'_i(m+1).\text{lat}}{d'_i(m).t - d'_i(m+1).t} \quad (7)$$

$$\beta'_{im,\text{lat}} = d'_i(m).\text{lat} - \alpha'_{im,\text{lat}} \times d'_i(m).t \quad (8)$$

$$\alpha'_{im,\text{lon}} = \frac{d'_i(m).\text{lon} - d'_i(m+1).\text{lon}}{d'_i(m).t - d'_i(m+1).t} \quad (9)$$

$$\beta'_{im,\text{lon}} = d'_i(m).\text{lon} - \alpha'_{im,\text{lon}} \times d'_i(m).t \quad (10)$$

(3) 線形補間を用いて、以下のようにして  $a'_i(n)$  を得る.

$$a'_i(n).\text{lat} = \alpha'_{im,\text{lat}} \times a'_i(n).t + \beta'_{im,\text{lat}} \quad (11)$$

$$a'_i(n).\text{lon} = \alpha'_{im,\text{lon}} \times a'_i(n).t + \beta'_{im,\text{lon}} \quad (12)$$

ただし、 $a'_i(n).t = a_j(n).t$  である.

(4)  $a'_i(n)$  と  $a_j(n)$  の緯度、経度からヒュベニの公式\*3を用いて、地理的距離  $L_{\text{geo}}(a'_i(n), a_j(n))$  を計測する.

(5) 以下のように、 $d'_i$  と  $a_j$  の距離  $L(d'_i, a_j)$  を定義する.

$$L(d'_i, a_j) \equiv \frac{\sum_{1 \leq n \leq |a_j|} L_{\text{geo}}(a'_i(n), a_j(n))}{|a_j|} \quad (13)$$

## 4. 実験準備

本節では、次節の実験に  $D$  として用いる2つの実データと、実験に先だてて行う前処理を紹介する. また、 $D$  を  $D'$  とする2つの匿名化手法について紹介する.

### 4.1 データ1: Cabspotting

$D$  として実験に用いる実データの1つ目は、Cabspotting データセット [21] である. このデータは、サンフランシスコにおける30日間の536台のタクシーの軌跡情報により構成されている. 位置情報レコードの総数は、11,219,955 となっている.

### 4.2 データ2: Geolife

2つ目の実データは、Geolife データセット [22] である. これは、182人の個人の軌跡情報を4年間に渡って収集したデータであり、24,876,978の位置情報レコードで構成されている.

### 4.3 データ前処理

上記2つのデータセットは、長期間における軌跡情報である. しかし、攻撃者が長期間に渡る軌跡情報を持ち合わせているとは限らないため、本稿は、ある時間間隔における連続的な軌跡について攻撃者が持ち合わせている背景知識と、匿名化され公開された軌跡情報の比較により、個人を再識別するリスクを評価する方法の提案に主眼を置いている. そこで前処理として、上記2つの実データを時間的に不連続なタイミングで軌跡情報を分断する. 具体的には、[8]に従い、ある個人の軌跡情報において隣り合う2つの位置情報の時刻が4時間以上差がある場合に、軌跡情報を分断し、別の個人として取り扱う. また、 $|d_i| \geq 3$  の軌跡情報のみ残す. 前処理して得られたデータセットの基本情報を表3に示す.

\*3 ヒュベニの公式は、2点間の距離が大きくなるほど、真の距離との誤差が広がるものであるが、本稿の範囲内では十分な精度である.

表3 前処理した実データの基本情報.

$D$	Cabspotting	Geolife
$ D $	11,219,925	24,876,940
$N_D$	6,860	16,032
1人当たり平均 $ d_i $	1,635.6	1,551.7
1人当たり平均収集時間間隔 (秒)	75.7	17.5

### 4.4 匿名化手法1: ノイズ付加

軌跡情報匿名化の1つとして、緯度、経度へノイズを付加することにより、個人特定性を低減する方法が考えられる. 本稿では、地表上における二次元ラプラス分布から生成した乱数により、緯度、経度へ確率的ノイズ付加を行う [8], [23]. より具体的には、以下の通りである.

原点に位置する二次元極座標ラプラス分布の確率分布関数は、

$$P_\epsilon(r, \theta) = \frac{\epsilon^2}{2\pi} r e^{-\epsilon r} \quad (14)$$

で与えられる. ここで、 $r$  は原点からある点の距離、 $\theta$  は原点とある点を結ぶ直線とデカルト座標における横軸との角度である.  $P_\epsilon(r, \theta)$  からランダムに生成した  $r, \theta$  は、以下のようにして緯度、経度に加算した.

$$d'_i(j).\text{lat} = d_i(j).\text{lat} + r \sin(\theta) / L_{\text{Per1degLat}} \quad (15)$$

$$L_{\text{Per1degLat}} = 2\pi R_E / 360 \quad (16)$$

$$d'_i(j).\text{lon} = d_i(j).\text{lon} + r \cos(\theta) / L_{\text{Per1degLon}} \quad (17)$$

$$L_{\text{Per1degLon}} = 2\pi R_E \cos(\pi d_i(j).\text{lat} / 180) / 360 \quad (18)$$

ここで、 $R_E$  は赤道半径であり、6,378,137mとした. このノイズ加算方法は、地球が球体であることを仮定しているが、本稿の範囲では十分な精度 (1%未満) であることを確認している. 本匿名化手法は、 $\epsilon$  がパラメータとなり、これが小さいほど与えるノイズ量は大きくなる.

### 4.5 匿名化手法2: サンプリング

一般的に、 $|d_i|$  が大きいほど  $d_i$  は多様になりやすく、再識別がより容易になる. したがって、 $d_i$  から位置情報レコードを一部抽出することは有効な手段の1つになりうると思われる. そこで本稿で用いる軌跡情報匿名化の2つ目として、ランダムなサンプリングを用いる. 抽出する数  $N_{\text{sample}}$  をパラメータとし、 $d_i$  からランダムに抽出し、 $d'_i$  とする. ただし、 $|d_i| \leq N_{\text{sample}}$  の場合は、 $d'_i = d_i$  とする.

### 4.6 生成した攻撃者の背景知識の誤差評価方法

3.1節で導入した攻撃者の背景知識の生成方法は、ある個人の2つの位置情報レコード間で緯度、経度が時刻の一次関数として記述できることを仮定している. この近似は、個人の移動速度に対して、位置情報収集の時間間隔が十分に小さい場合は有効であると考えられる. しかし、これはデータの性質により、結果的に線形近似に起因して真の軌

表 4 生成した攻撃者の背景知識  $A$  の誤差評価結果.

$D$	Cabspotting	Geolife
$L_{\text{error}}$ の平均値 [m]	157.1	18.9
$L_{\text{error}} < 10$ m の割合 (総数)	0.79% (54)	91% (14,549)

跡からのずれが生じる可能性があり、検証が必要である。そこで、本稿では以下に示す保守的な誤差評価を行い、誤差が十分に小さい  $a_i$  のみ攻撃者の背景知識として用いることとする。

具体的には、 $[d_i(j).t, d_i(j+2).t]$  の時間間隔で緯度、経度について線形補間を行い、 $d_i(j+1).t$  における緯度、経度を予測する。これら緯度、経度と真の値である  $d_i(j+1).lat$ ,  $d_i(j+1).lon$  との地理的距離を計測する。 $1 \leq j \leq |d_i| - 2$  のすべての  $j$  で、予測値と真値の距離を計り、その平均値を算出し、 $L_{\text{error}}$  とする。これが一般的な GPS 精度である 10 m 未満となる場合のみ、 $d_i$  から  $a_i$  を生成し、攻撃者の背景知識とする。提案している攻撃者の背景知識生成方法は、 $[d_i(j).t, d_i(j+1).t]$  というより狭い時間間隔で線形補間を行うため、この誤差評価は保守的であると言える。

## 5. 実験結果

本節では、実験結果を示す。なお実験環境は、OS: macOS 10.12, CPU: 1.1 GHz Intel Core m3, RAM: 8 GB, 使用言語: c++, コンパイラ: g++である。

### 5.1 生成した攻撃者の背景知識の誤差評価

まず、4.6 節で議論した攻撃者の背景知識の保守的な誤差評価について議論する。例として、図 1 に、Cabspotting データセットに含まれる  $|d_i| = 500$ ,  $L_{\text{error}} = 242.9$  m の  $d_i$  と、 $|a_i| = 16$  として  $d_i$  から生成した  $a_i$  を示す。図 2 には、Geolife データセットに含まれる  $|d_i| = 470$ ,  $L_{\text{error}} = 4.8$  m の  $d_i$  と、 $|a_i| = 16$  として  $d_i$  から生成した  $a_i$  を示す。

表 4 に定量的な評価結果を示す。Cabspotting データセットの方が、Geolife データセットに比べて誤差が大きくなっており、 $L_{\text{error}} < 10$  m となる割合もずっと低いことがわかる。これは、Cabspotting データセットがタクシーの軌跡情報であるにも関わらず、位置情報を収集する時間間隔が長いことにより、本稿が提案する簡素な線形補間を用いた手法では、攻撃者の背景知識  $A$  が真の軌跡から大きくずれてしまうことを意味していると考えられる。この結果から、Cabspotting データセットから十分に誤差が小さい  $a_i$  を、十分な個数生成することが難しいため、以降の実験では Geolife データセットのみ用いることとする。

### 5.2 匿名性評価

攻撃者の背景知識  $A$  を生成するためのパラメーターである攻撃者の背景知識量  $|a_i|$  は、すべての  $i$  に共通して、

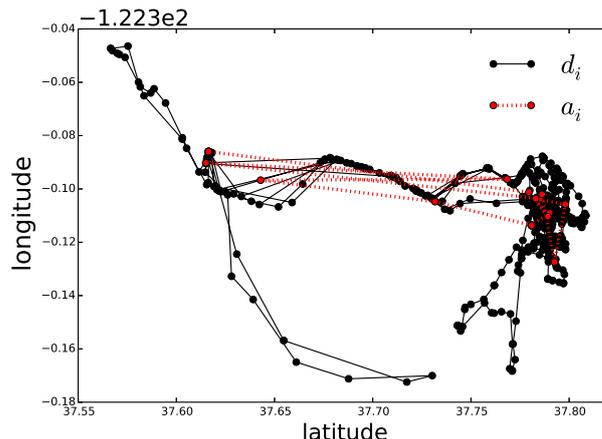


図 1 Cabspotting データセットに含まれる  $|d_i| = 500$ ,  $L_{\text{error}} = 242.9$  m の  $d_i$  と、 $|a_i| = 16$  として  $d_i$  から生成した  $a_i$  を例示。

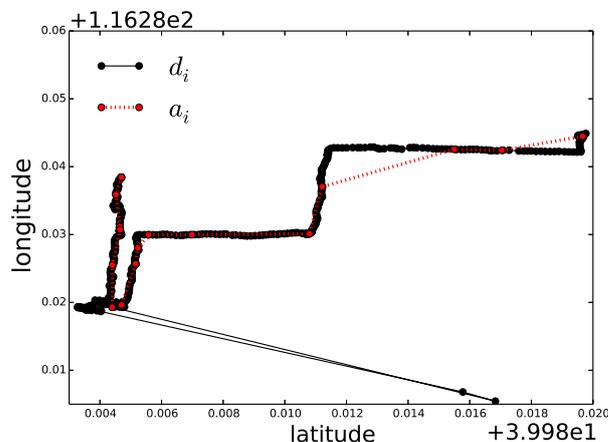


図 2 Geolife データセットに含まれる  $|d_i| = 470$ ,  $L_{\text{error}} = 4.8$  m の  $d_i$  と、 $|a_i| = 16$  として  $d_i$  から生成した  $a_i$  を例示。

$|a_i| = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024$  の 11 通りを採用する。全てのパラメーター値に対して 10 回、匿名化、 $A$  の生成と攻撃を実施し、再識別が成功した割合 (=再識別が成功した  $a_i$  の数  $N_A$ ) の 1 試行当たり平均と標準偏差を計算する。ただし計算量削減のため、1 試行ごとに  $A$  からランダムに 1,000 の  $a_i$  を抽出 (つまり  $N_A = 1000$ ) し、実験に用いる。 $D'$  は全体を用いるため、表 3 の  $N_D$  と同じく  $N_{D'} = 16032$  となる。

#### 5.2.1 匿名化手法 1

匿名化手法 1 では、 $\epsilon = \ln(2)/200$  として、匿名化を実施した。図 2 で示した  $a_i$  と、 $d_i$  を匿名化した  $d'_i$  を図 3 に示す。再識別が成功した割合を攻撃者の背景知識量パラメーター  $|a_i|$  の関数として図 4 に示す。比較として、匿名化しない場合 (つまり  $D' = D$ ) の再識別成功率を緑点線で示す。

#### 5.2.2 匿名化手法 2

匿名化手法 2 では、サンプルする個数  $N_{\text{sample}} = 2, 8$  とし

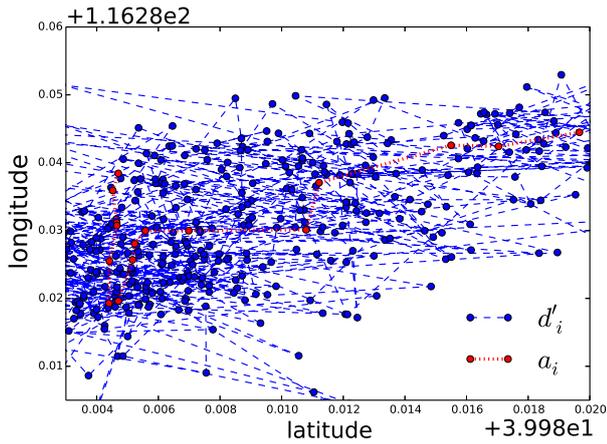


図3 図2で示した  $a_i$  と  $d_i$  を  $\epsilon = \ln(2)/200$  の匿名化手法1で匿名化した  $d'_i$  を例示.

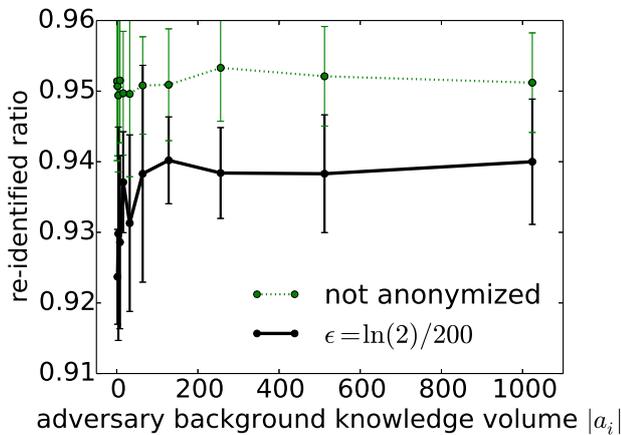


図4  $\epsilon = \ln(2)/200$  とした匿名化手法1で得られた  $D'$  の匿名性評価の結果. 個人特定が成功した割合を攻撃者の背景知識量パラメーター  $|a_i|$  の関数として表示. 緑点線は, 匿名化しない場合の再識別成功率を示す. 表示する値は, 10回の試行の平均, 誤差は, 標準偏差である.

て, 匿名化を行った. 図2で示した  $a_i$  と  $d_i$  を  $N_{\text{sample}} = 8$  の匿名化手法2で匿名化した  $d'_i$  を図5に示す. 再識別が成功した割合を攻撃者の背景知識量パラメーター  $|a_i|$  の関数として図6に示す.

### 5.2.3 議論

図4, 6ともに, 低  $|a_i|$  側では,  $|a_i|$  の増加につれ, 再識別成功率が上昇する傾向があるが, 高  $|a_i|$  側では成功率はほぼ一定である. このことは, 攻撃能力を強化するためには, ある程度の背景知識量が必要であるが, それを超えると攻撃能力が漸近することを示唆している.

図3から,  $\epsilon = \ln(2)/200$  の匿名化手法1で得られる  $d'_i$  は極めてノイズだということが見て取れる. 平均的な距離の誤差 (つまり  $r$  の平均値) は570 mほどに達する. また, [8]の筆者らは, 同じ  $\epsilon$  の値を用いて, Geolife データセットを匿名化し, POI (Point Of Interest) を抽出する攻撃を実施している. 結果, 抽出した POI の正確度は F-

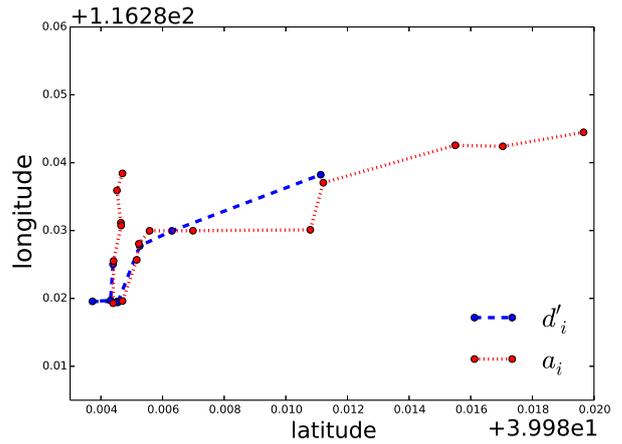


図5 図2で示した  $a_i$  と  $d_i$  を  $N_{\text{sample}} = 8$  の匿名化手法2で匿名化した  $d'_i$  を例示.

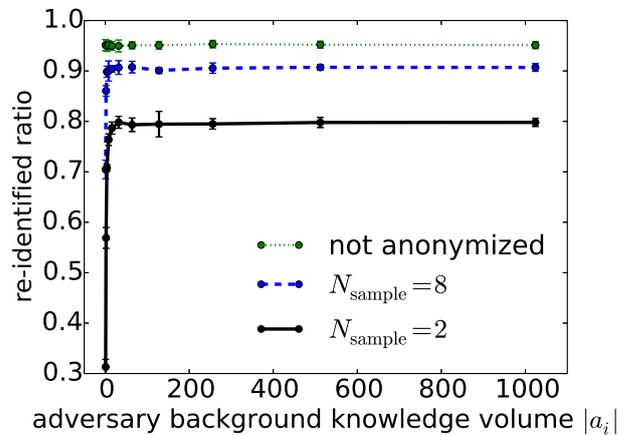


図6  $N_{\text{sample}} = 2, 8$  とした匿名化手法2で得られた  $D'$  の匿名性評価の結果. 個人特定が成功した割合を攻撃者の背景知識量パラメーター  $|a_i|$  の関数として表示. 緑点線は, 匿名化しない場合の再識別成功率を示す. 表示する値は, 10回の試行の平均, 誤差は, 標準偏差である.

値で0.85%であり, ほとんどまったく抽出できないと報告している. これらのことから, 加工の度合いとしては非常に大きいものであると考えられる. しかし, 図4からは,  $|a_i| = 1$  を含むすべての場合で, 再識別成功率は91%を超え, 高い割合であることがわかる. また11中7の  $|a_i|$  の値において, 匿名化をしていない場合 ( $D' = D$ ) の再識別成功率と誤差の範囲で一致する. したがって, 本稿で提案した攻撃者モデルに対しては, Geolife データセットのノイズ付加による匿名性向上の効果は極めて限定的であるといえる.

一方, 図6より, サンプル数  $N_{\text{sample}} = 2, 8$  の匿名化手法2は, 匿名化無しの場合や匿名化手法1より低い再識別成功率を与えることがわかる. したがって Geolife データセットは, 本稿で提案した攻撃者モデルに対して, サンプルリングが匿名性を向上させるより有効な手段と言える. しかし,  $N_{\text{sample}} = 2$  でも依然再識別成功率は  $|a_i| \geq 16$  で

80%ほどに達する。加えて元々平均で1,000以上の $|d_i|$ が2まで大幅に低減されることになってしまい、元の特徴がほとんど維持されていないと考えられ、この点においても課題が残る。

## 6. まとめ

本稿では、匿名化され公開された軌跡情報から、個人が再識別されるリスクに対して、攻撃者モデルに基づく匿名性評価方法を提案した。

この攻撃者モデルは、背景知識生成方法と攻撃手法の2つからなる。背景知識生成は、ある時間帯におけるある個人の軌跡情報を取得できるのは1つの事業者に限らないという軌跡情報の性質に基づき、簡素な線形補間を用いて元データ $D$ から現実的な背景知識 $A$ を生成するものである。攻撃手法は、匿名化データ中の軌跡 $d'_i$ と背景知識中の軌跡 $a_j$ の距離を計測することにより、個人を強力に再識別するものである。

提案した匿名性評価法で、2つの匿名化手法（ノイズ付加、サンプリング）で得られた匿名化データ $D'$ の匿名性を評価する実験も行った。元データ $D$ としては、実際の軌跡情報であり、十分な精度で攻撃者の背景知識 $A$ を生成できるGeolifeデータセットを用いた。その結果、本稿で提案した攻撃者モデルに対して、Geolifeデータセットの匿名性を向上させるには、ノイズ付加よりも位置情報レコードのサンプリングの方が効果的であることがわかった。このように匿名化して得られたデータ $D'$ に対して、現実的な攻撃者モデルに基づき、匿名性を向上するためにはどのような匿名化が適切なかの判断できるという点に、本稿で提案した匿名性評価方法の重要性がある。

今後の課題として、攻撃者の背景知識 $A$ の生成方法の高精度化がある。本稿では、元データ中の2つの時刻の間で、緯度、経度を時刻の一次関数として近似した。このことに起因して、Cabspottingデータセットでは十分な精度で攻撃者の背景知識 $A$ を生成することができなかったと考えられる。 $A$ の精度向上のためには、道路の情報を事前情報として用いて近似に用いる関数をより最適なものにすることが考えられる。この課題が解決されれば、より多様なデータセットを匿名性評価の実験に用いることができ、再識別を防ぐ軌跡情報匿名化手法についてより一般的な知見が得られることが期待できる。

謝辞 軌跡情報の実データセットを公開してくださった[21]、[22]の著者の方々に深く感謝いたします。

## 参考文献

- [1] L. Sweeney, “ $k$ -Anonymity: A Model for Protecting Privacy,” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems archive, Volume 10 Issue 5, October 2002, Pages 557 - 570
- [2] D. Ikarashi, R. Kikuchi, K. Chida, K. Takahashi, “k-Anonymous Microdata Release via Post Randomisation Method,” 10th International Workshop on Security, IWSEC 2015, Nara, Japan, August 26-28, 2015, Proceedings, pp 225-241
- [3] C. Dwork, “Differential privacy,” ICALP’06 Proceedings of the 33rd international conference on Automata, Languages and Programming - Volume Part II Pages 1-12
- [4] O. Abul, F. Bonchi, and M. Nanni, “Never walk alone: Uncertainty for anonymity in moving objects databases,” In Proceedings of the IEEE International Conference on Data Engineering, 2008.
- [5] M. E. Nergiz et al., “Towards trajectory anonymization: A generalization-based approach,” Transactions on Data Privacy, 2(1):47-75, 2009.
- [6] 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.
- [7] K. Jiang, D. Shao, S. Bressan, T. Kister, and K.-L. Tan, “Publishing Trajectories with Differential Privacy Guarantees,” in Proceedings of the 25th International Conference on Scientific and Statistical Database Management. ACM, 2013, pp. 12:1-12:12.
- [8] V. Primault, S. B. Mokhtar, C. Lauradoux and L. Brunie, “Time Distortion Anonymization for the Publication of Mobility Data with High Utility,” 2015 IEEE Trustcom/BigDataSE/ISP, 2015.
- [9] 正木彰伍, 長谷川聡, 千田浩司, 「時空間におけるクラスタリングを用いた軌跡情報の $k$ -匿名化法」, コンピュータセキュリティシンポジウム 2016 論文集, 2016(2), pp.921-928, 2016.
- [10] 正木彰伍, 「時空間クラスタリングを用いた軌跡情報 $k$ -匿名化法の位置精度向上に関する考察」, 暗号と情報セキュリティシンポジウム SCIS 2017 予稿集, 3A4-4, 2017.
- [11] Philippe Golle and Kurt Partridge. 2009. On the Anonymity of Home/Work Location Pairs. In Proceedings of the 7th International Conference on Pervasive Computing (Pervasive '09), Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Brush, and Yoshito Tobe (Eds.), Springer-Verlag, Berlin, Heidelberg, 390-397.
- [12] Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux. 2011. Evaluating the privacy risk of location-based services. In Proceedings of the 15th international conference on Financial Cryptography and Data Security (FC'11), George Danezis (Ed.). Springer-Verlag, Berlin, Heidelberg, 31-46.
- [13] Yoni De Mulder, George Danezis, Lejla Batina, and Bart Preneel. 2008. Identification via location-profiling in GSM networks. In Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES '08). ACM, New York, NY, USA, 23-32.
- [14] Sbastien Gambs, Marc-Olivier Killijian, and Miguel Nez Del Prado Cortez. 2014. De-anonymization attack on geolocated data. J. Comput. Syst. Sci. 80, 8 (December 2014), 1597-1614.
- [15] Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. 2011. Quantifying Location Privacy. In Proceedings of the 2011 IEEE Symposium on Security and Privacy (SP '11). IEEE Computer Society, Washington, DC, USA, 247-262.
- [16] T. Murakami, A. Kanemura, H. Hino, “Group Sparsity Tensor Factorization for Re-Identification of Open Mobility Traces,” IEEE Transactions on Information Forensics and Security, Volume: 12, Issue: 3, March 2017.
- [17] 菊池 浩明, 山口 高康, 濱田 浩気, 山岡 裕司, 小栗 秀暢, 佐

- 久間 淳, 「匿名加工・再識別コンテスト Ice & Fire の設計」, コンピュータセキュリティシンポジウム 2015 論文集, 2015(3), pp.363-370, (2015).
- [18] 菊池 浩明, 小栗 秀暢, 野島 良, 濱田 浩気, 村上 隆夫, 山岡 裕司, 山口 高康, 渡辺 知恵美, 「PWSCUP: 履歴データを安全に匿名加工せよ」, コンピュータセキュリティシンポジウム 2016 論文集, 2016(2), pp.271-278, (2016).
- [19] H. Kikuchi, T. Yamaguchi, K. Hamada, Y. Yamaoka, H. Oguri and J. Sakuma, "Ice and Fire: Quantifying the Risk of Re-identification and Utility in Data Anonymization," 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, 2016, pp. 1035-1042.
- [20] T. Murakami, "Quantifying the Risk of Re-identification in Data Anonymization Competition", WODIAC workshop, 2017.
- [21] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "CRAWDAD data set epfl/mobility (v. 2009-02-24)," Downloaded from <http://crawdad.cs.dartmouth.edu/epfl/mobility>
- [22] Y. Zheng, X. Xie, and W.-Y. Ma, "GeoLife: A Collaborative Social Networking Service among User, location and trajectory," IEEE Data Engineering Bulletin, vol. 33, no. 2, pp. 32-40, 2010.
- [23] M. E. Andres, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential Privacy for Location-based Systems," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013, pp. 901-914.