

推薦論文

背景知識を用いて移動履歴から個人を特定する 確率モデルの提案と評価

松本 瞬^{1,a)} 大岡 拓斗¹ 市野 将嗣¹ 吉浦 裕¹

受付日 2021年2月6日, 採録日 2021年5月11日

概要：個人の位置情報は、携帯電話会社や位置情報サービスの提供者により収集され、産業界や公共分野で有効活用されている。一方、移動履歴にはプライベートな情報が含まれているため、これを保護するために匿名加工処理を行ったうえで利活用するのが一般的である。しかし、匿名加工を施した移動履歴とは異なる別データを参照し、これらと匿名移動履歴を対応付けることで、匿名性を解除する攻撃が多数提案されている。この攻撃の1つとして、遷移情報に基づいた攻撃が存在するが、既存手法は匿名移動履歴および対応付けを行うための別データ以外の活用ができていない。近年は、スマートフォンなどの普及にともなって大量の位置情報が取得可能になっており、これらを背景知識として活用することで、従来の攻撃精度を超えた攻撃が可能となりうる。そこで本論文では、大量の位置情報を背景知識として利用可能な攻撃モデルを数学的に導いた。また、この手法を実装したうえで、2種類のデータセットを用いて評価実験を行い、既存手法と比較した。これにより、背景知識のデータ量が増えるにつれて提案手法の攻撃成功率が上昇し、データ量が十分な量に達したとき、既存手法の攻撃成功率を上回ることを明らかにした。

キーワード：プライバシーリスク, 移動履歴, 再特定, ソーシャルネットワークサービス

Proposal and Evaluation of a Probabilistic Model that Identifies an Individual from the Location History Using Background Knowledge

SHUN MATSUMOTO^{1,a)} TAKUTO OOKA¹ MASATSUGU ICHINO¹ HIROSHI YOSHIURA¹

Received: February 6, 2021, Accepted: May 11, 2021

Abstract: Personal location histories are collected by cell phone companies and location-based service providers, and these information is effectively used in industry and the public sector. On the other hand, since location histories contain private information, it is common to use them after anonymized processing to protect. However, a number of attacks have been proposed to break the anonymity by referring to other data that is different from the anonymized location histories and mapping them to the anonymized location histories. One of these attacks is based on transition information, but the existing methods do not make use of anything other than anonymous location histories and data for mapping to them. In recent years, with the spread of smartphones and other devices, a large amount of location history can be obtained, so by using this information as background knowledge, attacks that exceed the accuracy of conventional attacks may become possible. In this paper, we mathematically derive an attack model that can use a large amount of location information as background knowledge. We also implement the proposed method, and conducted evaluation experiments using two different datasets and compared the results with existing methods. Then, we found that the success rate of the proposed method increases as the amount of background knowledge data increases, and when the amount of data reaches a sufficient level, the success rate of the proposed method exceeds that of the existing methods.

Keywords: privacy risk, location history, re-identification, social network service

¹ 電気通信大学
The University of Electro-Communications, Chofu, Tokyo
182-8585, Japan
^{a)} matsushun3182@gmail.com

本論文の内容は2020年3月の第88回CSEC研究会にて報告され、同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である。

1. はじめに

位置情報を時系列で記録した移動履歴は、携帯電話会社や位置情報サービスの提供者によって大量に収集されている。特に近年は、GPS を内蔵したスマートフォンの普及、またスマートフォン上で動作する位置情報を扱ったアプリケーションの出現により、より多様な事業者が位置情報を収集できるようになっている。こうして得られる位置情報を活用することで、サービス内でのレコメンドの最適化や地点の自動タグ付けなど、サービスの質の向上に期待ができる。また、これらのデータを研究機関や調査会社のような第三者へ提供して解析することで、交通システムの改善や災害時の避難計画など、公共分野での活用も可能になる。

一方で、移動履歴には個人の機微な情報（自宅や通勤通学先、個人の生活習慣など）が含まれているので、ストーカー犯罪などにつながる可能性がある。そのため、移動履歴を利用する際は、仮名化・曖昧化・ノイズ付加などの匿名加工処理を行い、機密情報を保護するのが一般的である。しかし、匿名加工を施した移動履歴とは異なる別データ（以下、サイドデータという）を参照し、これらと匿名移動履歴を対応付けることで、匿名性を解除する攻撃が多数提案されている。匿名性解除攻撃の1つとして、マルコフ連鎖モデルに基づいた攻撃が存在する [1], [2]。これらの手法では、サイドデータとして得られる個人の移動履歴（以下、実名移動履歴という）からユーザごとの移動傾向を学習し、これらと匿名移動履歴を対応付けることで、匿名移動履歴の匿名性を解除する。

近年は、スマートフォンなどの普及にともなって大量の位置情報が取得可能になっており、これらの位置情報を背景知識として用いることで、高い精度での匿名性の解除が可能となりうる。しかし、既存の匿名性解除手法では背景知識を用いていない。本論文では、背景知識の活用が可能な攻撃モデルを導出することで、既存手法の問題を解決できる新たな手法を提案する。また、性質の異なる2つのデータセットを用いて実験し、既存手法と比較することで、その有用性を明らかにする。

2. 先行研究

2.1 概要

移動履歴のプライバシーに対する攻撃には、特定の時刻に存在していた位置を推定する攻撃（Localization Attacks）[1], [2]、ユーザ間の接触を推定する攻撃（Meeting Disclosure Attacks）[1]、目的地を推定する攻撃 [3], [4]、ユーザの属性を推定する攻撃 [5] などがあるが、ここではサイドデータとの照合をとおして匿名移動履歴の仮名性を解除する攻撃（以下、再特定という）について述べる。

移動履歴の再特定攻撃は、グラフの照合による方式 [6], [7], [8]、滞在情報に基づく方式 [9], [10], [11]、遷

表 1 既存手法の分類

Table 1 Classification of existing methods.

方式	手法	特徴
グラフ	Srivatsa ら [6] Ji ら [7]	SNS の交友関係を利用
	Manousakas ら [8]	地理的情報必要なし
	Unnikrishnan ら [9] Murakami [10] Riederer ら [11]	滞在分布間の照合 行列分解による補完 滞在回数の分布を仮定
遷移	Gambs ら [12] Shokri ら [1]	地点のクラスタリング Gibbs サンプリングによる補完
	Murakami [2]	EM アルゴリズム・テンソル分解による補完
ノイズ分布	Ma ら [13]	地理的ノイズの分布を仮定

移情報に基づく方式 [1], [2], [12]、地理的ノイズの確率分布に基づく方式 [13] という分類ができる。各既存手法の分類を表 1 に示す。

以下では、方式の分類に沿って論じることとし、最初にグラフの照合による方式を述べる。Srivatsa らや Ji らは、匿名移動履歴間の接触関係グラフとソーシャルネットワークサービス（以下、SNS という）上での交友関係グラフを照合し、匿名移動履歴と SNS アカウントを対応付けることにより、再特定を行った [6], [7]。Manousakas らは、匿名移動履歴、実名移動履歴それぞれについて、場所をノード、場所間の遷移をエッジとするグラフを作成し、グラフ間の照合によって各移動履歴を対応付け、再特定を行った [8]。Manousakas らの手法は、位置情報に緯度・経度といった地理的情報が付随していない状態であっても利用可能である点が特徴的である。Manousakas らの手法以外は、位置情報に地理的情報が付随していることを前提としている。

次に滞在情報に基づく方式について述べる。Unnikrishnan らや Murakami は、実名移動履歴と匿名移動履歴それぞれについて、ユーザごとの滞在分布を作成し、各々の滞在分布を照合することで再特定を行った [9], [10]。滞在分布とは、地点ごとの滞在比率を記録したものである。これらの手法では、時刻を離散化したうえで、地点ごとの滞在時刻数をカウントし、これらを合計時刻数で割ることで、滞在分布を作成している。Murakami の手法については、滞在分布の作成後に行列分解を行うことで、位置情報数の少ない実名移動履歴からの学習を可能にしている。Riederer らは、異なる2つのサービスの利用履歴をもとに作成した移動履歴から、ユーザが同じ移動履歴のペアを推定した [11]。地点ごとの滞在回数がポアソン分布に従うとし、（移動履歴のペアが同一ユーザであると仮定した場合の移動履歴の生起確率）/（移動履歴のペアが異なるユーザであると仮定した場合の移動履歴の生起確率）を対象ペアの類似度として用いることで、ユーザが同一である移動履歴のペアを推定

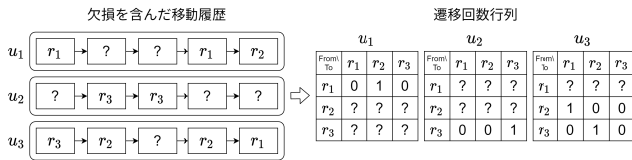


図 1 欠損を含んだ移動履歴からの学習の例

Fig. 1 Example of learning from location history that has missing location.

している。なお、この手法は事前学習に Unnikrishnan らの手法 [9] を用いている。

遷移情報に基づく方式について述べる。Gambs らは、実名移動履歴と匿名移動履歴それぞれについて、ユーザーごとの遷移確率行列 (2 地点間を遷移する確率を各要素として持つ行列) を作成し、各々の遷移確率行列を対応付けることで再特定を行った [12]。Shokri らや Murakami は、位置情報の欠損を含んだ実名移動履歴から、位置情報を補完しながら遷移確率行列を作成し、遷移確率行列と匿名移動履歴を対応付けることで、再特定を行った [1], [2]。

最後に、地理的ノイズの確率分布に基づく方式について述べる。Ma らは、地理的近接性に基づいて実名移動履歴と匿名移動履歴の相違度を計算し、これをもとに再特定を行った [13]。この手法では、匿名移動履歴に加わる地理的ノイズの分布を仮定したうえで、位置情報の地理的近接性に基づいた相違度計算式を定式化した。

2.2 類似研究

本節では、提案手法と類似した、遷移情報に基づく再特定の手法について詳しく述べる。

Gambs らの手法 [12] では、実名移動履歴と匿名移動履歴それぞれについて、ユーザーごとの遷移確率行列を作成する。その後、様々な行列間類似度指標を用いて類似度を計算し、実名移動履歴の遷移確率行列と匿名移動履歴の遷移確率行列を対応付けることで再特定を行う。なおこの手法では、移動履歴の取得対象地域に含まれる地点について事前にクラスタリングしている。地点が持つ属性 (たとえば、家・職場など) ごとにクラスタリングしたうえで、そのクラスター間の遷移に関する遷移確率行列を作成している。Gambs らの手法の問題点として、位置情報の欠損を考慮していない点があげられる。実名移動履歴は、位置情報サービスや SNS などを通して得る必要があるが、これらの手段では完全な移動履歴を入手するのは難しく、位置情報の欠損が発生することが一般的である。位置情報の欠損が発生した場合、図 1 のように、入手した移動履歴そのものから遷移回数行列 (2 地点間の遷移回数を各要素として持つ行列) を作成することが困難になる。Gambs らの手法では、この問題に対処できない。

Shokri らは、遷移確率行列の作成で用いる実名移動履歴に位置情報の欠損があることを考慮し、この欠損を補完し

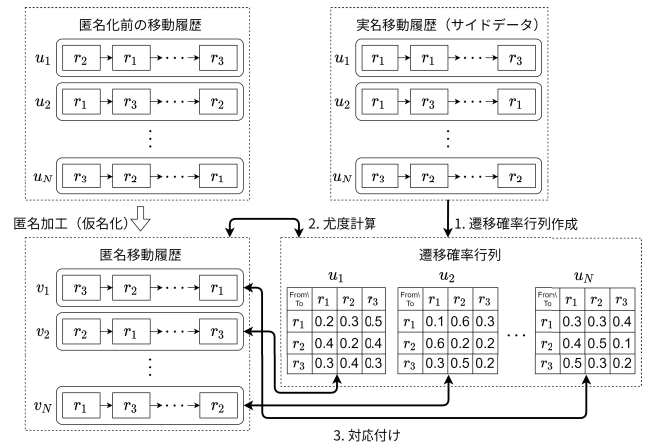


図 2 Shokri らの手法の攻撃の流れ

Fig. 2 Attack flow of Shokri et al.'s method.

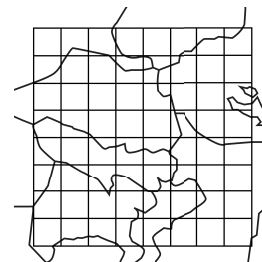


図 3 メッシュ分割の例

Fig. 3 Example of mesh division.

ながら遷移確率行列を作成する手法を提案した [1]。この手法の流れは図 2 のようになっている。まず移動履歴の取得対象地域を図 3 のような一定サイズのメッシュに分割し、実名移動履歴からメッシュ間の遷移確率行列を作成する。その後、各遷移確率行列をもとに各匿名移動履歴の尤度を計算し、これを類似度とすることで、遷移確率行列と匿名移動履歴を対応付け、再特定を行う。この手法では、実名移動履歴から遷移確率行列を作成する際に Gibbs サンプリングを用いることで、欠損した位置情報を補完する。これにより、Gambs らの手法では実現できなかった、位置情報の欠損の考慮が可能になる。

Murakami は、遷移確率行列の作成に用いる実名移動履歴について、

- 位置情報の欠損がある
- 入手できる位置情報数が少ない

ことを想定した遷移確率行列の作成手法を提案した [2]。この手法は EM アルゴリズムに基づいており、テンソル分解を併せて用いることで、欠損部分の考慮及び再特定対象のユーザー間に共通した特徴の活用を実現している。これにより、上記 2 つの性質を持つ移動履歴から遷移確率行列を作成可能とした。

2.3 背景知識の利用

近年は、スマートフォンなどの普及・発展にともない、

表 2 記号の表記
Table 2 Notations.

記号	説明
U	実名移動履歴のユーザ集合
V	匿名移動履歴のユーザ集合
N	ユーザ数
σ	U から V への対応関係を示す関数
$\mathcal{R}$	移動履歴の観測地域
$\mathcal{T}$	移動履歴の観測期間
S_u	ユーザ u の実名移動履歴
L_v	ユーザ v の匿名移動履歴
S	実名移動履歴の集合
L	匿名移動履歴の集合

大量の位置情報が取得可能になっている。たとえば、投稿に位置情報のタグ付けができる SNS から投稿を収集すれば、大量の位置情報を取得できる。また、位置情報サービスを提供している企業や携帯会社、Wi-Fi 基地局設置企業であれば、より正確な位置情報を大量に入手可能である。これらのデータを背景知識として有効利用することで、再特定の新たなアプローチを開拓できる可能性がある。

Shokri らは、位置情報取得対象地域の地形情報を把握するために、遷移確率行列の作成時に背景知識を利用することを示唆している。しかし、Shokri らはこの方法を具体化していない。また、その他の既存手法については背景知識の活用を想定していない。

提案方式では、大量の位置情報を背景知識として利用可能な枠組みを提案する。これにより、既存手法の精度を超えた再特定を目指す。

3. 提案方式

3.1 記号の表記

ある地域 $\mathcal{R}$ において、実名移動履歴と匿名移動履歴が観測される。実名移動履歴のユーザ集合を $\{u_1, \dots, u_N\} \in U$ とし、匿名移動履歴のユーザ集合を $\{v_1, \dots, v_N\} \in V$ とする。本方式では、実名移動履歴と匿名移動履歴を元にユーザ間の対応関係 $\sigma: U \rightarrow V$ を明らかにすることを目的とする。

移動履歴について、詳細に定義する。移動履歴はユーザごとに存在しており、ユーザ u の実名移動履歴を S_u 、ユーザ v の匿名移動履歴を L_v と表記する。また、移動履歴は、複数の位置情報から構成されている。実名移動履歴の位置情報は、ユーザ $u \in U$ 、時刻 $t \in \mathcal{T}$ 、地点 $r \in \mathcal{R}$ からなるタプル (u, t, r) で表現する。匿名移動履歴の位置情報も同様にタプル (v, t, r) で表現する。すなわち、ユーザ u の実名移動履歴は $S_u = ((u, t_1, r_1), (u, t_2, r_2), \dots)$ と表現される。簡単のため、以降はユーザ u の k 番目の位置情報 (u, t_k, r_k) を $S_u(k)$ と表記することとする。また、移動履歴に含まれる位置情報の件数は $|S_u|$ と表記し、この値はユーザごとに

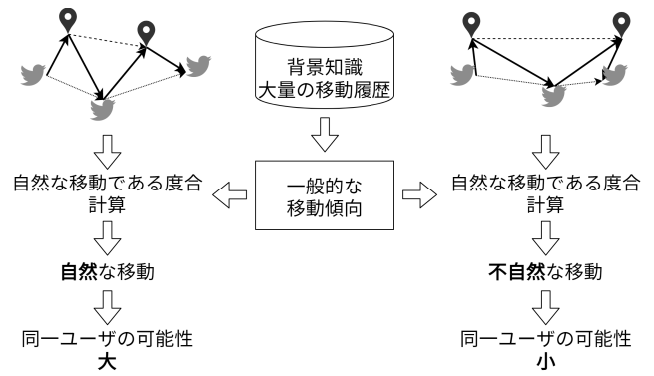


図 4 提案方式の基本アイデア

Fig. 4 Basic idea of the proposed method.

異なる。さらに、実名移動履歴の集合を $S = \{S_u \mid u \in U\}$ 、匿名移動履歴の集合を $L = \{L_v \mid v \in V\}$ と表記する。

3.2 基本アイデア

本方式は、「実名移動履歴のユーザ u と匿名移動履歴のユーザ v が同一であるとき、ユーザ u の移動履歴とユーザ v の移動履歴を結合してできる移動履歴は、地域 $\mathcal{R}$ において自然な移動履歴になる」という仮定に基づいて構築する。学習ステップでは、背景知識から地域 $\mathcal{R}$ における自然な移動履歴の傾向を学習する。このステップでの目的は、ユーザごとの移動傾向を学習することではなく、一般的な移動傾向を学習することである。そのため、再特定対象のユーザ集合 U, V とは関係のない、大量の移動履歴（以下、移動履歴ビッグデータという）を背景知識として学習データに使用できる。照合ステップでは、図 4 のように、学習ステップで得られた一般的な移動傾向を用いて、結合移動履歴がどれだけ自然な移動履歴であるかを計算する。この値が大きければ大きいほど、同一ユーザらしさが高いと見なす。これをユーザの組合せ全通りについて計算し比較することで、実名移動履歴と匿名移動履歴の間の対応関係を明らかにし、再特定を行う。

3.3 基本理論

1. 実名移動履歴の集合 S
2. 匿名移動履歴の集合 L
3. 一般的な移動傾向 θ

の 3 つが与えられたもとでの、 $u \in U$ と $v \in V$ が同一ユーザである確率 $P(u \equiv v \mid S, L, \theta)$ を定式化する。ここで、 $u \equiv v$ は u と v が同一ユーザである事象を示している。本方式では、以下を仮定して理論を展開する。

$$P(u \equiv v) = \frac{1}{N} \quad (\forall u \in U, \forall v \in V) \quad (1)$$

$$P(u \equiv v \mid \theta) = P(u \equiv v) \quad (2)$$

$$P(S, L \mid \theta, u \equiv v) \\ = P(S_u, L_v \mid \theta, u \equiv v)$$

$$\cdot \prod_{u' \in U, u' \neq u} P(S_{u'} | \theta) \cdot \prod_{v' \in V, v' \neq v} P(L_{v'} | \theta) \quad (3)$$

式 (1) は、事前情報がないとき、ユーザ u, v が同一である確率は $1/N$ で一定であることを意味している。式 (2) は、ユーザ u, v の移動履歴に関する情報がない限り、一般的な移動傾向 θ のもとであっても、ユーザ u, v が同一である確率は依然として $1/N$ であることを意味している。式 (3) は、あるユーザ u, v が同一であると判明している場合の移動履歴発生確率の計算方法を示している。 u, v については同一ユーザであるため同時確率を計算し、それ以外のユーザについては独立に移動履歴の発生確率を計算する。これらを掛け合わせたものが、全移動履歴の同時発生確率 $P(S, L | \theta, u \equiv v)$ と等しくなる、と仮定する。

上記の 3 つの仮定を用いることで、 $u \in U$ と $v \in V$ が同一ユーザである確率 $P(u \equiv v | S, L, \theta)$ は次のように変形できる。

$$\begin{aligned} P(u \equiv v | S, L, \theta) &= \frac{P(S, L, \theta | u \equiv v) \cdot P(u \equiv v)}{\sum_{(u', v') \in U \times V} P(S, L, \theta | u' \equiv v') \cdot P(u' \equiv v')} \\ &= \frac{P(S, L | \theta, u \equiv v) \cdot P(\theta) \cdot P(u \equiv v)}{\sum_{(u', v') \in U \times V} P(S, L | \theta, u' \equiv v') \cdot P(\theta) \cdot P(u' \equiv v')} \\ &\propto P(S, L | \theta, u \equiv v) \\ &= P(S_u, L_v | \theta, u \equiv v) \\ &\quad \cdot \prod_{u' \in U, u' \neq u} P(S_{u'} | \theta) \cdot \prod_{v' \in V, v' \neq v} P(L_{v'} | \theta) \\ &\propto \frac{P(S_u, L_v | \theta, u \equiv v)}{P(S_u | \theta) \cdot P(L_v | \theta)} \end{aligned} \quad (4)$$

1 行目から 2 行目への変形にはベイズの定理を用いた。また、2 行目から 3 行目への変形には式 (2) の仮定に基づいて得られる式 (5) の変形を用いた。

$$\begin{aligned} P(S, L, \theta | u \equiv v) &= \frac{P(S, L | \theta, u \equiv v) \cdot P(\theta, u \equiv v)}{P(u \equiv v)} \\ &= \frac{P(S, L | \theta, u \equiv v) \cdot P(u \equiv v | \theta) \cdot P(\theta)}{P(u \equiv v)} \\ &= \frac{P(S, L | \theta, u \equiv v) \cdot P(u \equiv v) \cdot P(\theta)}{P(u \equiv v)} \\ &= P(S, L | u \equiv v, \theta) \cdot P(\theta) \end{aligned} \quad (5)$$

3 行目から 4 行目への変形では、式 (1) の仮定を用いた。4 行目から 5 行目への変形では、式 (3) の仮定を用いた。6 行目の式は、5 行目の式を $\prod_{u' \in U} P(S_{u'}) \cdot \prod_{v' \in V} P(L_{v'} | \theta)$ で割ることにより得られる。 $\prod_{u' \in U} P(S_{u'}) \cdot \prod_{v' \in V} P(L_{v'} | \theta)$ は S, L, θ のみから決まる値であり、 u, v に依存しないため、5 行目と 6 行目の式の間で比例の関係が保たれる。

以上により得られる式 (4) を、 u と v の類似度 $D(u, v)$ として用いる。

$$D(u, v) = \frac{P(S_u, L_v | \theta, u \equiv v)}{P(S_u | \theta) \cdot P(L_v | \theta)} \quad (6)$$

アルゴリズム 1 σ の推定

Require: S, L , 移動履歴ビッグデータ

```

1: 移動履歴ビッグデータから一般的な移動傾向  $\theta$  を学習
2: for  $(u, v) \in (U \times V)$  do
3:    $S_u, L_v, \theta$  を用いて  $D(u, v)$  を計算
4: end for
5:  $E \leftarrow \{D(u, v) : (u, v) \in (U \times V)\}$ 
6:  $\sigma \leftarrow$  二部グラフ  $B(U, V, E)$  について、最大重みマッチング問題を解く
7: return  $\sigma$ 

```

3.4 処理の流れ

類似度 $D(u, v)$ を用いて、ユーザの対応関係 σ を明らかにするための手順を示す。ユーザの対応関係 σ を推定する際の全体の流れはアルゴリズム 1 のようになっている。まず、移動履歴ビッグデータから一般的な移動傾向 θ を学習する。その後、ユーザの組合せ全通り分について、類似度 $D(u, v)$ を計算する。最後に、 $D(u, v)$ を辺の重みとした二部グラフについて、最大重みマッチング問題を解くことで、実名移動履歴と匿名移動履歴の間の対応関係 σ を求める。なお、最大重みマッチング問題を解く処理にはハンガリアン法 [14] を用いた。

4. 方式の具体化

本章では、アルゴリズム 1 の具体化を行う。本手法では、移動傾向 θ として、Shokri ら [1] や Murakami [2] が使用していた遷移確率行列を使用する。遷移確率行列とは、観測地域 $\mathcal{R}$ を $r'_1, \dots, r'_{R'} \in \mathcal{R}'$ の R' 個の小地域に分割したときの、小地域間の遷移確率を保持する $R' \times R'$ の行列である。遷移確率行列の使用にともない、各位置情報の地点情報には、地点 r の代わりに、該当地点 r が属する小地域 r' を使用することとする。

本手法における遷移確率行列 θ の作成方法を図 5 に示す。手順は次のとおりである。

(1) 背景知識として用いる移動履歴ビッグデータについて、各位置情報に含まれる地点情報 r を図 3 のようにメッシュ分割し、小地域 $r' \in \mathcal{R}'$ に変換する

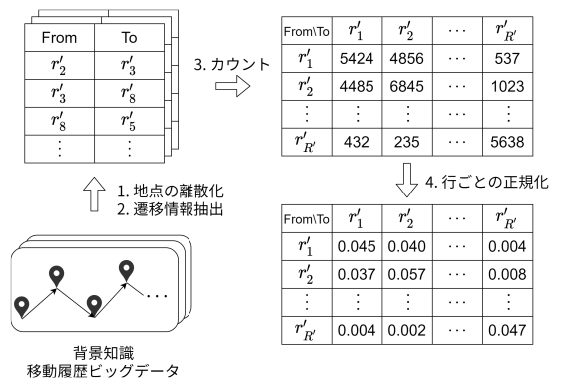


図 5 遷移確率行列 θ の作成方法

Fig. 5 How to create a transition probability matrix θ .

表 3 データセットの統計情報

Table 3 Statistics of datasets.

データセット	移動履歴の種類	ユーザ数	1人あたりの 平均位置情報数	1人あたり1日あたりの 平均位置情報数	期間
Foursquare	S, L	500	116.88	1.82	2012-04-25–2013-01-29
	移動履歴ビッグデータ	1,500	241.41	3.07	2012-04-04–2013-02-16
Twitter - Wi-Fi	S (Twitter 移動履歴)	50	40.40	1.63	2017-01-25–2017-04-24
	L (Wi-Fi 移動履歴)	50	12,721.36	170.47	2017-01-25–2017-04-24
	移動履歴ビッグデータ	300,000	118.16	1.95	2007-04-24–2017-06-26

- (2) 移動履歴から小地域間の遷移情報を抽出する
 (3) 各遷移の発生回数をカウントし、遷移回数行列を作成する
 (4) 行の和が1になるように正規化を行い、遷移確率行列を作成する

なお 3.2 節で述べたように、ここで使用する移動履歴ビッグデータはユーザ個別の移動傾向を学習するためのものではない。そのため、移動履歴は仮名化済みのものであってよい。

次に、類似度 $D(u, v)$ の計算方法を具体化する。本手法では、式 (1), (2), (3) に加えて、以下を仮定する。

$$P((w, t, r) | \theta) = \text{const.} \quad (\forall w \in U, V) \quad (7)$$

$$P(H_w(k) | H_w(k-1), \dots, H_w(1), \theta) \\ = P(H_w(k) | H_w(k-1), \theta) \quad (\forall H_w \in S, L) \quad (8)$$

$$P(S_u, L_v | \theta, u \equiv v) = P(M_{(u,v)} | \theta) \quad (9)$$

式 (7) は、任意の時刻・地点について、滞在確率が一定であることを表している。これは、遷移確率行列 θ が滞在確率に関する情報を有していないことを考慮しており、妥当な仮定になっている。式 (8) では、任意の移動履歴について、発生確率がマルコフ性を満たすことを仮定している。式 (9) は、ユーザが同一であるときの2つの移動履歴の発生確率の計算方法を示している。 $M_{(u,v)}$ は、図 4 における実線の矢印のような、移動履歴 S_u と移動履歴 L_v を結合してできる移動履歴を意味している。この結合移動履歴 $M_{(u,v)}$ は、2つの移動履歴 S_u, L_v に含まれる位置情報を1つにまとめ、時刻順に並べ替えることで作られる移動履歴であり、 $M_{(u,v)}$ の位置情報数 $|M_{(u,v)}|$ は $|S_u| + |L_v|$ になる。式 (9) では、ユーザが同一であるときの2つの移動履歴の発生確率が、結合移動履歴 $M_{(u,v)}$ の発生確率と等しくなることを仮定している。

以上の仮定を用いると、類似度計算式は次のように変形できる。

$$D(u, v) \\ = \frac{P(S_u, L_v | \theta, u \equiv v)}{P(S_u | \theta) \cdot P(L_v | \theta)} \\ = \frac{P(M_{(u,v)} | \theta)}{P(S_u | \theta) \cdot P(L_v | \theta)}$$

表 4 移動履歴の観測範囲

Table 4 Observation range of location history.

データセット	最東端 (東経)	最西端 (東経)	最南端 (北緯)	最北端 (北緯)
Foursquare	139.9126 度	139.4709 度	35.5102 度	35.8672 度
Twitter - Wi-Fi	140.4003 度	138.9999 度	35.2515 度	36.3923 度

$$\propto \frac{\prod_{k=2}^{|M_{(u,v)}|} P(M_{(u,v)}(k) | M_{(u,v)}(k-1), \theta)}{\prod_{k=2}^{|S_u|} P(S_u(k) | S_u(k-1), \theta) \cdot \prod_{k=2}^{|L_v|} P(L_v(k) | L_v(k-1), \theta)} \quad (10)$$

各確率値 $P(H_w(k) | H_w(k-1), \theta)$ には、遷移確率行列 θ 内の該当遷移の値を使用する。

5. データセット

本手法の有用性を評価するために、2種類のデータセットを用意した。1つは Foursquare のオープンデータを元に作成したデータセット、もう1つは我々が独自に収集したデータセットである。それぞれのデータセットの統計情報、観測範囲情報は表 3, 表 4 のようになっている。本章ではそれぞれのデータセットの詳細について説明する。なお、本データセットでは、実名移動履歴 S と匿名移動履歴 L の位置情報の取得対象期間が同一であるが、移動パターンが定型的である場合、位置情報の取得対象期間が同一である必要はないと考えられる。

5.1 Foursquare データセット

位置情報を利用した SNS である Foursquare から収集したデータセットを用いる [15]。本データセットには 2012 年 04 月 04 日から 2013 年 02 月 16 日の間に観測された、2,293 人分の東京都内における位置情報が含まれている。なお、Foursquare は位置情報を扱うことを軸とした SNS であるため、位置情報に含まれる誤差については、5.2.1 項や 5.2.3 項で後述する疑似移動履歴と比べると小さいと考えられる。

5.1.1 実名移動履歴 S

まず、2,293 人のうち 500 人をランダム抽出し、これを再特定の対象ユーザとした。その後、対象ユーザの移動履歴について、各位置情報のランダム抽出によって移動履歴を 2 分割する。こうして得られた移動履歴のうち、一方を実名移動履歴 S とした。なお、移動履歴の期間については、

多くのユーザが共通して観測されている 2012 年 04 月 25 日から 2013 年 01 月 29 日までの 280 日間を対象とした。

5.1.2 匿名移動履歴 L

5.1.1 項で 2 分割して得られた移動履歴のうち、もう一方を匿名移動履歴 L とした。移動履歴の期間は、5.1.1 項と同様である。

5.1.3 移動履歴ビッグデータ

5.1.1, 5.1.2 項で再特定の対象に選ばなかったユーザのうち、1,500 人分の移動履歴を遷移確率行列 θ の学習で使用する移動履歴ビッグデータとした。移動履歴の期間については、2012 年 04 月 04 日から 2013 年 02 月 16 日を対象とした。

5.2 Twitter - Wi-Fi データセット

5.2.1 実名移動履歴 S

まず、本学の学生 22 人と一般の実験参加者 28 人、合わせて 50 人の Twitter アカウントの投稿文を取得した。こうして得られた投稿文のうち、地名を含むものだけを取り出し、その地名を緯度・経度に変換したうえで投稿時刻を付け加えることで、疑似的な移動履歴を作成し、これを実名移動履歴 S とした。なお、地名の変換処理には GeoNLP [16] と呼ばれるジオパースエンジンを用いている。移動履歴の取得対象期間は 2017 年 01 月 25 日から 2017 年 04 月 24 日までの 90 日間である。また、移動履歴の観測地域は東京都、神奈川県、千葉県、埼玉県と、これらに隣接した県の一部となっている。

このようにして得られる位置情報には、正確でないものが多く含まれている。正確でない位置情報の例として、次のような場合が存在する^{*1}。

- (1) 投稿時刻以外の時刻に当該地名の場所に存在していた。
例：「昨日は渋谷で遊んでいた」
- (2) 実際には存在していなかった地点を抽出してしまう。
例：「立川に住みたい」
- (3) GeoNLP 内の形態素解析処理の誤りにより、地名ではない単語（人名や会社名など）が誤検知される。
例：「藤沢くんは元気？」

5.2.2 匿名移動履歴 L

Wi-Fi 事業者の協力を得て、実名移動履歴 S と同一のユーザ 50 人のスマートフォンが Wi-Fi アクセスポイントに発したプローブ要求の記録から移動履歴を取得し^{*2}、こ

れを匿名移動履歴 L とした。移動履歴の取得対象期間と観測地域は実名移動履歴 S と同様である。ただし、スマートフォンの電源や Wi-Fi 機能を一時的にオフにしたユーザがいたため、全ユーザについて 90 日分の移動履歴を取得してはいない。また、プローブ要求は約 100 m 以内の Wi-Fi アクセスポイントに無線で到達するため、地点情報に関しては最大で 100 m 程度の誤差がある。

5.2.3 移動履歴ビッグデータ

まず、5.2.1 項で取得した 50 人分の Twitter アカウントとは関係のない、30 万人分の Twitter アカウントから投稿文を取得した。その後、5.2.1 項と同様の処理を施すことで、30 万人分の疑似的な移動履歴を作成し、これを遷移確率行列 θ の学習で使用する移動履歴ビッグデータとした。移動履歴ビッグデータについては、2017 年 06 月 26 日を起点に、過去にさかのぼって取得しており、取得対象期間は 2007 年 04 月 24 日から 2017 年 06 月 26 日となっている。なお、本移動履歴についても、5.2.1 項と同様に正確でない位置情報が多く含まれていると考えられる。

6. 評価

6.1 評価方法

3.4 節で述べた処理の流れにしたがって実装した。本論文では 2 種類の評価実験を行う。1 つ目の評価実験では、移動履歴ビッグデータに含まれるユーザ数と再特定成功率の関係を調べる。Twitter - Wi-Fi データセットでは、移動履歴ビッグデータ内のユーザ 300,000 人の中から、ランダムに 1, 10, 100, 1,000, 10,000, 100,000 人を抽出し、これをもとに遷移確率行列 θ を作成した際の成功率を調べる。Foursquare データセットでは、同様に 1,500 人のユーザの中から、ランダムに 1, 15, 150, 500, 1,000, 1,500 人を抽出し、これをもとに遷移確率行列 θ を作成した際の成功率を調べる。

2 つ目の評価実験では、実名移動履歴に対して意図的に欠損を発生させたときの再特定成功率について調べる。この際、Shokri らの手法では位置情報の欠損を補完しながら再特定を行う。移動履歴ビッグデータのユーザ数については、Twitter - Wi-Fi データセットでは 100,000 人、Foursquare データセットでは 1,500 人に固定する。

Foursquare データセットについては、2,293 人分の移動履歴から再特定の対象となる 500 人分の移動履歴を抽出する処理や、再特定対象の移動履歴を 2 分割する処理にランダム性が存在する。また、両方のデータセットについて、1 つ目の評価実験の際、移動履歴ビッグデータの中から一定のユーザ数を抽出する処理にランダム性が存在する。そのため、実験は条件ごとに 20 回ずつ行い、これらの平均を取った値をもとに評価した。

また、4 章で述べたように、提案手法では遷移確率行列を用いる際、観測地域 $\mathcal{R}$ を複数の小地域に分割する必要が

^{*1} 本データセットは松本ら [17] が実験で使用しているデータセットを元に作成している。松本らは、本文中 (1)–(3) に該当する投稿がそれぞれ 13.4%, 11.0%, 16.7%, 計 41.1% 存在したと述べている。本データセットは、松本ら [17] のデータセットに対し、対象期間を縮小する処理と、位置情報が極端に少ないユーザを削除する処理を施したのとなっているため、同じ比率を厳密に維持しているわけではないが、正確でない位置情報が多く含まれていると考えられる。

^{*2} 実験参加者からは個別に明確な事前同意を得たうえで、移動履歴の取得を行った。また、本研究は電気通信大学の倫理委員会の審査を経て実施している。

ある．本実験では，観測地域を $16 \times 16 = 256$ 分割し，遷移確率行列を作成した．分割後の小地域の 1 辺の長さは，Foursquare データセットでは縦 275 m，横 163 m，Twitter - Wi-Fi データセットでは縦 7,910 m，横 6,508 m となった．

6.2 比較対象

提案手法との比較対象として，遷移確率行列を用いた手法のなかで標準的な位置づけにある Shokri らの手法 [1] を採用することにした．Shokri らの手法についても実装し，提案手法の再特定成功率と比較する．Shokri らの手法の処理内容は次のとおりである．

- (1) 欠損補完済みの実名移動履歴 $ES_u^{\{l-1\}}$ をもとに遷移確率行列 $P^{\{l\}}$ をサンプリングする．サンプリングは遷移確率行列の行単位で行う．サンプリングを行う際に使用する分布は次の式によって生成される．

$$\text{Dirichlet} \left(\{ TC_{i,j} + \text{Cnt}_{i,j} (ES_u^{\{l-1\}}) + \epsilon_{ij} \}_{j=1..M} \right)$$

$\text{Cnt}_{i,j}(\cdot)$ は，小地域 r'_i から小地域 r'_j へ遷移した回数を意味している．また， TC_{ij} や $\epsilon_{i,j}$ は背景知識をもとに生成する値であるが，Shokri らはその生成方法を具体化していない．そのため，本実験ではこれらを考慮せずに $\text{Cnt}_{i,j}(\cdot)$ の値のみから分布を生成する．

- (2) 遷移確率行列 $P^{\{l\}}$ をもとに実名移動履歴 S_u の補完を行い，欠損補完済みの実名移動履歴 $ES_u^{\{l\}}$ を作成する．補完は $k = 1, \dots, |S_u|$ について逐次的に行う．次の式により小地域に関する確率分布を生成し，この分布からサンプリングを行うことで，補完後の小地域を決定する．

$$\frac{P_{ES_u(k-1), ES_u(k)}^{\{l\}} b(S_u(k) | ES_u(k)) P_{ES_u(k), ES_u(k+1)}^{\{l\}}}{\sum_{r' \in \mathcal{R}'} P_{ES_u(k-1), (u, t_k, r')}^{\{l\}} b(S_u(k) | (u, t_k, r')) P_{(u, t_k, r'), ES_u(k+1)}^{\{l\}}}$$

なお， $P_{ES_u(0), ES_u(1)}^{\{l\}}$ と $P_{ES_u(|S_u|), ES_u(|S_u|+1)}^{\{l\}}$ は 1 であるとする．また， b は次のように定義する．

$$b(S_u(k) | (u, t_k, r')) = \begin{cases} 0 & (r' \neq \emptyset \text{ and } r' \neq ES_u(k)) \\ 1 & (\text{otherwise}) \end{cases}$$

- (3) (1) と (2) を一定回数繰り返すことで， $(P^{\{l\}}, ET^{\{l\}})$ のペアを得る．
- (4) 遷移確率行列 $P^{\{l\}}$ の平均をとり，最終的な遷移確率行列 P を得る．
- (5) 遷移確率行列 P をもとに匿名移動履歴 L_v の尤度を計算する処理を，遷移確率行列 P と匿名移動履歴 L_v の組合せ全通り分について行う．
- (6) 尤度を重みとした二部グラフについて，最大重みマッチング問題を解くことで，実名移動履歴 S_u と匿名移動履歴 L_v を対応付ける．

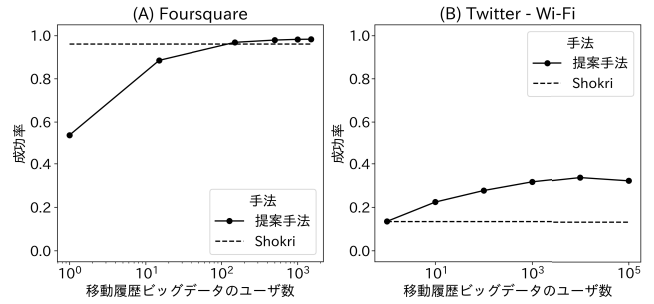


図 6 移動履歴ビッグデータのユーザ数と成功率の関係

Fig. 6 Relationship between the number of users of location history big data and the correct answer rate.

6.3 評価結果

6.3.1 移動履歴ビッグデータのユーザ数と成功率の関係

本項では，移動履歴ビッグデータに含まれるユーザ数を変化させたときの再特定成功率の変化について述べる．Foursquare データセットにおける実験結果を図 6 (A) に，Twitter - Wi-Fi データセットにおける実験結果を図 6 (B) に示す．なお，Shokri らの手法については，移動履歴ビッグデータを使用しないため，移動履歴ビッグデータのユーザ数に関わらず一定の成功率になっている．

まず，Foursquare データセットの実験結果について述べる．図 6 (A) から分かるとおり，提案手法については，移動履歴ビッグデータのユーザ数の増加にともなって成功率が上昇していることが分かる．移動履歴ビッグデータのユーザ数が 1, 15 人の段階では，Shokri らの手法の成功率のほうが高いが，150 人になった段階で Shokri らの手法の成功率を上回る．以降の 500, 1,000, 1,500 人ではさらに成功率が上昇している．しかし，移動履歴ビッグデータのユーザ数が 1, 15, 150 人のときと比べると，成功率の上昇の度合いは小さくなっている．

Foursquare データセットにおける実験結果について考察する．移動履歴ビッグデータのユーザ数が 1 人であるとき，Shokri らの手法は提案手法の成功率を上回っている．これは，Shokri らの手法が再特定対象のユーザごとに移動傾向を学習するからであると考えられる．提案手法は，再特定の対象とは異なるユーザから一般的な移動傾向を学習するのに対し，Shokri らの手法では，再特定の対象となるユーザの移動傾向を直接学習する．そのため，再特定対象のユーザの移動傾向を 1 人 1 人詳細に把握できる Shokri らの手法に分があると考えられる．移動履歴ビッグデータのユーザ数が 15 人の場合についても，同様の理由から Shokri らの手法の成功率のほうが高い．しかし，移動履歴ビッグデータのユーザ数が 150 人になると提案手法が Shokri らの手法の成功率を上回る．移動履歴ビッグデータのユーザ数が十分な数に達すると，提案手法の移動履歴ビッグデータによる効果が，先述した Shokri らの手法の効果を上回り，提案手法が有利になると考えられる．

次に、Twitter - Wi-Fi データセットの実験結果について述べる。Twitter - Wi-Fi データセットについても、図 6 (B) から分かるとおり、移動履歴ビッグデータのユーザ数増加にともなって成功率が上昇している。こちらのデータセットでは、ユーザ数が 10,000 人に達するまで成功率が上昇してる。一方、Shokri らの手法の成功率は低く、移動履歴ビッグデータのユーザ数が 1 人のときと同等の成功率となっている。

Twitter - Wi-Fi データセットにおける実験結果について考察する。Shokri らの手法は、Foursquare データセットでの結果とは異なり、低い成功率となっている。これは、5.2.1 項で述べたように、実名移動履歴に相当する Twitter 移動履歴が、1 人あたりの位置情報数が少ない、かつ誤差を含んでいるという性質を有しているためであると考えられる。先述したように、Shokri らの手法では、実名移動履歴からユーザの移動傾向を直接学習する。このとき、実名移動履歴の位置情報数が少ない場合や、位置情報が正確でない場合は、移動傾向の十分な学習ができない。Twitter - Wi-Fi データセットはこれらの性質を有しており、移動傾向の学習が困難であるため、低い成功率になったと考えられる。提案手法についても、移動履歴ビッグデータのユーザ数が少ない場合は、十分な学習ができず、低い成功率になっている。しかし、ユーザ数が膨大な数に増えることで、位置情報の少なさや不正確さによる悪影響が軽減され、正確な移動傾向の学習が可能になっていると考えられる。

いずれのデータセットにおいても、移動傾向の学習に十分な移動履歴ビッグデータのユーザ数が確保できた段階で、提案手法は Shokri らの手法の成功率を上回っている。そのため、移動履歴ビッグデータの活用は、移動履歴の再特定において有効であるといえる。特に、位置情報数が少ない場合や位置情報が正確でない場合には、移動履歴ビッグデータによる成功率上昇の効果は大きくなると考えられる。

6.3.2 位置情報の欠損率と成功率の関係

本項では、実名移動履歴の位置情報を欠損させたときの再特定成功率について述べる。Foursquare データセットにおける実験結果を図 7 (A) に、Twitter - Wi-Fi データセットにおける実験結果を図 7 (B) に示す。図 7 から分かるとおり、どちらのデータセットについても、任意の欠損率において、提案手法の成功率が Shokri らの手法の成功率を上回っている。特に、Foursquare データセットでは、欠損率が大きくなるにつれて、Shokri らの手法の成功率が大幅に低下している。これは、位置情報数の大幅な減少により、Gibbs サンプルングによる補完処理を施した場合でも、移動傾向の学習が困難になったためであると考えられる。提案手法については、移動履歴ビッグデータから移動傾向を学習しているため、実名移動履歴の位置情報欠損による影響が小さく、成功率の低下を抑えることができています。

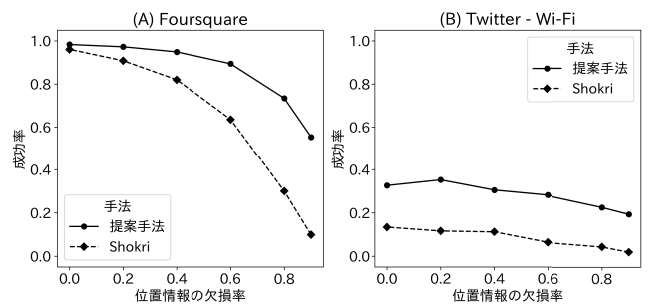


図 7 位置情報の欠損率と成功率の関係

Fig. 7 Relationship between loss rate of location history and correct answer rate.

7. まとめ

本論文では、移動履歴の再特定攻撃として、移動履歴ビッグデータが利用可能な手法を提案した。既存手法では、再特定の対象となる移動履歴の位置情報数が少ない場合、移動傾向の学習が困難になり、再特定の精度が低下していた。そこで、本手法では、再特定対象の移動履歴から移動傾向を学習するのではなく、移動履歴ビッグデータから一般的な移動傾向を学習し、これを用いて類似度を計算することで、位置情報数が少ない場合にも対応できるようにした。また、移動履歴ビッグデータから得られた一般的な移動傾向を、変数として類似度計算式に組み込むことで、理論的な正当性も明らかにした。

実験では、2 種類のデータセットに対して再特定を行った。一方は、実験参加者 500 人について、Foursquare から得られた位置情報を元に作成した移動履歴のセットである。移動履歴ビッグデータには、Foursquare から得られた 1,500 人分の移動履歴を用意した。もう一方は、実験参加者 50 人について、Twitter 上の投稿を元に作成した移動履歴と、Wi-Fi 基地局から得られた移動履歴のセットである。移動履歴ビッグデータには、Twitter 上の投稿を元に作成した 30 万人分の移動履歴を用意した。これらのデータセットを用いて実験した結果、移動履歴ビッグデータに含まれるユーザ数が増えれば増えるほど正解率が上昇した。また、移動履歴に対して意図的に位置情報の欠損を発生させたうえで実験した結果、提案手法が Shokri らの手法より高い正解率を発揮した。これは、移動履歴ビッグデータを用いたことの効果によるものだと考えられる。

提案手法は理論的な正当性を確保したうえで、移動履歴ビッグデータの利用を可能にしておき、実験においても既存手法の精度を上回っている。このことから、提案手法は既存手法と比べてより有用な手法であるといえる。

参考文献

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

- (2011).
- [2] Murakami, T.: Expectation-maximization tensor factorization for practical location privacy attacks, *Proc. Privacy Enhancing Technologies*, Vol.2017, No.4, pp.138–155 (2017).
 - [3] Monreale, A., Pinelli, F., Trasarti, R. and Giannotti, F.: Wherenext: A location predictor on trajectory pattern mining, *Proc. 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp.637–646 (2009).
 - [4] Xue, A.Y., Zhang, R., Zheng, Y., Xie, X., Huang, J. and Xu, Z.: Destination prediction by sub-trajectory synthesis and privacy protection against such prediction, *2013 IEEE 29th International Conference on Data Engineering (ICDE)*, pp.254–265, IEEE (2013).
 - [5] Matsuo, Y., Okazaki, N., Izumi, K., Nakamura, Y., Nishimura, T., Hasida, K. and Nakashima, H.: Inferring Long-term User Properties Based on Users' Location History, *IJCAI*, pp.2159–2165 (2007).
 - [6] Srivatsa, M. and Hicks, M.: Deanonymizing mobility traces: Using social network as a side-channel, *Proc. 2012 ACM Conference on Computer and Communications Security*, pp.628–637, ACM (2012).
 - [7] Ji, S., Li, W., Gong, N.Z., Mittal, P. and Beyah, R.A.: On Your Social Network De-anonymizability: Quantification and Large Scale Evaluation with Seed Knowledge, *NDSS* (2015).
 - [8] Manousakas, D., Mascolo, C., Beresford, A.R., Chan, D. and Sharma, N.: Quantifying privacy loss of human mobility graph topology, *Proc. Privacy Enhancing Technologies*, Vol.2018, No.3, pp.5–21 (2018).
 - [9] Unnikrishnan, J. and Naini, F.M.: De-anonymizing private data by matching statistics, *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp.1616–1623, IEEE (2013).
 - [10] Murakami, T.: A succinct model for re-identification of mobility traces based on small training data, *2018 International Symposium on Information Theory and Its Applications (ISITA)*, pp.164–168, IEEE (2018).
 - [11] Riederer, C., Kim, Y., Chaintreau, A., Korula, N. and Lattanzi, S.: Linking users across domains with location data: Theory and validation, *Proc. 25th International Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, pp.707–719 (2016).
 - [12] Gambs, S., Killijian, M.-O. and del Prado Cortez, M.N.: De-anonymization attack on geolocated data, *Journal of Computer and System Sciences*, Vol.80, No.8, pp.1597–1614 (2014).
 - [13] Ma, C.Y., Yau, D.K., Yip, N.K. and Rao, N.S.: Privacy vulnerability of published anonymous mobility traces, *Proc. 16th Annual International Conference on Mobile Computing and Networking*, pp.185–196 (2010).
 - [14] Kuhn, H.W.: The Hungarian method for the assignment problem, *Naval Research Logistics Quarterly*, Vol.2, No.1-2, pp.83–97 (1955).
 - [15] Yang, D., Zhang, D., Zheng, V.W. and Yu, Z.: Modeling user activity preference by leveraging user spatial temporal characteristics in LBSNs, *IEEE Trans. Systems, Man, and Cybernetics: Systems*, Vol.45, No.1, pp.129–142 (2015).
 - [16] 国立情報学研究所: GeoNLP - 文章を自動的に地図化する地名情報処理システム, 国立情報学研究所 (オンライン), 入手先 (<https://geonlp.ex.nii.ac.jp/>) (参照 2021-02-07).
 - [17] 松本 瞬, 大岡拓斗, 市野将嗣, 吉浦 裕: 対象者の人

数と対象者間の関係に制約のない移動履歴とソーシャルネットワークの照合方式, 情報処理学会論文誌, Vol.61, No.12, pp.1814–1830 (2020).

推薦文

本論文は、移動履歴からの個人特定に関する研究である。個人情報が Wi-Fi など収集される時代にあって SNS の利用によって現実には起きうる個人特定の問題を扱っており、従来研究にない「自然な移動」という独自の観点を導入し、移動履歴の位置情報数が少ない場合にも対応可能なモデルを提案し、実装およびデータセットを用いて評価を行い、かつ現実的に適用可能な範囲での推定結果を得ている。以上のことから、推薦論文に値するため、推薦いたします。

(コンピュータセキュリティ研究会主査 山内利宏)

松本 瞬



2019 年電気通信大学情報理工学部総合情報学科卒業。2021 年電気通信大学情報理工学研究科情報学専攻博士前期課程修了。

大岡 拓斗



2019 年電気通信大学情報理工学部総合情報学科卒業。2021 年電気通信大学情報理工学研究科情報学専攻博士前期課程修了。現在、株式会社野村総合研究所勤務。

市野 将嗣 (正会員)



2003 年早稲田大学理工学部電子・情報通信学科卒業。2008 年同大学大学院理工学研究科博士課程修了。2007 年日本学術振興会特別研究員。2009 年早稲田大学大学院基幹理工学研究科研究助手。2010 年同大学メディアネットワークセンター助手。2011 年電気通信大学大学院情報理工学研究科助教。2016 年同大学大学院情報理工学研究科准教授。バイオメトリクス、ネットワークセキュリティに関する研究に従事。博士 (工学)。電子情報通信学会会員。



吉浦 裕 （正会員）

1981 年東京大学理学部情報科学科卒業。日立製作所勤務後、電気通信大学情報理工学研究科教授を経て、現在、京都橘大学工学部教授。情報セキュリティ、プライバシー保護の研究に従事。

博士（理学）。日立製作所社長技術賞（2000 年）、情報処理学会論文賞（2005 年，2011 年）、日本セキュリティ・マネジメント学会論文賞（2010 年，2016 年，2018 年）、システム制御情報学会産業技術賞（2005 年）、IEEE IHH-MSP best paper award（2006 年）、IFIP I3E best paper award（2016 年）等受賞。電子情報通信学会，日本セキュリティ・マネジメント学会，人工知能学会，システム制御情報学会，IEEE 各会員。本会フェロー。