欠損位置情報の推定を伴うテンソル分解と個人識別攻撃への応用

村上 隆夫 †

† 産業技術総合研究所 情報技術研究部門
135-0064 東京都江東区青海 2-3-26 産業技術総合研究所 臨海副都心センター
takao-murakami@aist.go.jp

あらまし 個人毎に学習したマルコフ遷移行列を基に，匿名化されたトレース（移動軌跡）から個人を識別する攻撃（個人識別攻撃）が提案されている．しかし，個人が普段から公開する位置情報は一般的に多くなく，また一定時間おきに公開するとも限らない．この場合，学習に使用できるトレースは少量で，かつ一部の位置情報が欠損し得る．本稿では，この状況下でも頑健に遷移行列を推定するため，Viterbi アルゴリズムを用いた欠損位置情報の推定と，テンソル分解を用いた個人毎の遷移行列の学習を繰り返す学習法を提案する．この学習法を個人識別攻撃に適用し，最尤推定，及び Gibbs サンプリングを用いた学習法との比較を通して，有効性を示す．

Tensor Factorization with Missing Location Estimation and Its Application to De-anonymization Attacks

Takao Murakami†

†Information Technology Research Institute (ITRI),
National Institute of Advanced Industrial Science and Technology (AIST)
AIST Tokyo Waterfront, 2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, Japan
takao-murakami@aist.go.jp

Abstract Recent studies have proposed de-anonymization attacks for mobility traces using personalized transition matrices. However, since many users only disclose a small amount of location data in their daily lives, the number of training traces can be very small. Also, since they do not disclose their locations at a fixed interval, missing locations can exist in the training traces. To address these issues, we propose a learning method that iterates estimating missing locations using the Viterbi algorithm and estimating transition matrices using tensor factorization. We show its effectiveness through a comparison with conventional learning methods.

1 はじめに

スマートフォンやカーナビゲーションシステムの普及に伴い，周辺の飲食店などの POI（Point of Interest）検索や，目的地への経路検索といった「位置情報サービス」（LBS: Location-based Service）が広く利用されている．その結果，大量のトレース（位置情報を時系列に並べた移動軌跡）がデータセンター側に蓄積されるようになり，「位置情報ビッグデータ」（Spatial Big Data）[1] として様々な用途に利活用されることが期待されている．例えば，大量のトレースを第三者提供することで，燃費効率の良い経路の分析 [1] や，旅行者が興味を持つ場所の分析 [2] などが可能となる．或いは，ユーザのクエリに応じてトレースを地図上に可視化することで（即ち，不特定多数の人々に公開することで），道路交通情報をユーザに提供することもできる [3].

しかし，トレースを第三者提供する（或いは公開する）ことによって，個人のプライバシー

が侵害される恐れがある．例えば，そのトレースを基に，自宅や通院している病院などが特定される恐れがあり，さらには秘密にしておきたい交友関係，趣味嗜好などが推測される恐れもある．従って，トレースを収集した事業者（LBSプロバイダーなど）が第三者提供をする（或いは公開する）際には，氏名などの「直接識別子」（Explicit Identifier）を削除して，トレースを匿名化する必要がある．一方，この対策だけでは不十分であることも指摘されている．具体的には，匿名化されたトレース（以後，匿名化トレース）から個人を識別する「個人識別攻撃」（De-anonymization Attack）[4–9] が，幅広く研究されている（言い換えれば，トレースそのものが，個人を特定し得る「準識別子」（Quasi-Identifier）になっている）．

個人識別攻撃として最も代表的なアプローチの一つが，マルコフモデル（Markov Model）に基づく手法である [6–9]．この手法では，まず人々が移動可能な領域を計 M 個の領域 $x_1, \cdots, x_M$ に分割することで（或いは人々が頻繁に訪れる計 M 個の POI のみを対象とすることで），位置情報を離散化する．時間についても，予め定められた時間間隔（30 分，1 時間など）おきに区切って離散化する．その上で，人々の行動にマルコフ性を仮定し，攻撃対象とする個人毎に，領域 x_i（$1 \leq i \leq M$）から次の時刻に領域 x_j（$1 \leq j \leq M$）に遷移する確率で構成される $M \times M$ の遷移行列を学習する．文献 [6, 7] は，この遷移行列の学習に利用できる（個人と紐付いた）トレース（以後，学習用トレース）が大量にある場合に，この手法が約 50% 以上の高い精度で個人を識別できることを示している．

しかし，個人が普段から（SNS などで）公開している位置情報は一般には多くなく（1 日に数回など），また一定時間おきに位置情報を公開するとも限らないことに注意が必要である．即ち，遷移行列の学習に利用できるトレースは，現実には少量であり，かつ一部の位置情報が欠損し得る．文献 [6–9] では各個人の遷移行列を独立に学習しているが，この場合，学習データが不足して遷移行列が正しく学習できない恐れがある．この学習データ不足の問題は，従来ではほとんど議論されていない．

筆者らは，学習用トレースが少量の場合でも遷移行列を頑健に学習するため，テンソル分解（Tensor Factorization）[10,11] を用いた遷移行列の学習法を提案している [12,13]．これは，個人毎の遷移行列の集合を 3 次元テンソルと見做し，低ランクな行列の積に分解して学習を行うものである．文献 [12] と文献 [13] は，この学習法をそれぞれ位置予測攻撃（ユーザが公開した位置情報を基に，その後の位置を予測する攻撃）と個人識別攻撃に適用し，最尤推定 [6–8] との比較を通して有効性を示している [1]．しかし，文献 [12, 13] では，学習用トレースから一部の位置情報が欠損する状況は考慮していない．

本稿の目的は，学習用トレースが少量で，かつ一部の位置情報が欠損するという現実的な状況において，個人識別攻撃の脅威の度合いを明確化することである．この目的を実現するため，本稿では，学習用トレースにおける欠損位置情報を推定しながら，テンソル分解を用いて遷移行列を学習する学習法を提案する．

本研究の貢献：

本研究の貢献は以下のとおりである．

- (a) 遷移行列を用いて欠損位置情報を Viterbi アルゴリズム [14] により推定し，(b) 推定した欠損位置情報を基に，遷移行列をテンソル分解を用いて学習し直す，ということを繰り返す学習法を提案する（第 5 章）．
- この提案手法を個人識別攻撃に適用し，最尤推定 [6–8]，及び Gibbs サンプリングを用いた学習法 [9] との比較を行い，提案手法の有効性を示す（第 6 章）．

記号の定義：

以下，本稿で用いる記号を定義する．攻撃対象とする個人の集合を $\mathcal{U} = \{u_1, \cdots, u_N\}$（計 N 人）とし，移動可能な領域（或いは POI）の集合を $\mathcal{X} = \{x_1, \cdots, x_M\}$（計 M 個）とする．時刻は一定時間おきに区切って離散化し，整数値で表す（即ち，時刻の集合は $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$）．ユーザ $u_n \in \mathcal{U}$ が領域 $x_i \in \mathcal{X}$ から次の時刻に領域 $x_j \in \mathcal{X}$ に遷移する確率を $p_{n,i,j}$ とし，ユーザ $u_n \in \mathcal{U}$ の遷移行列を P_n とする．このとき，個人毎の遷移行列の集合は，$\{P_n | n \in [N]\}$ と表せる（但し，$[N] = \{1, \cdots, N\}$）．

[1] 尚，文献 [13] では，位置情報がある種の「グループ構造」（例えば，都会／田舎エリア内に滞在する確率は一般に高い／低い，など）を持っていることに着眼し，これを捉えるためにグループスパース正則化（group sparsity regularization）をテンソル分解に組み込んだ学習法も提案している．本稿では簡単のため，そこまでは扱わない．

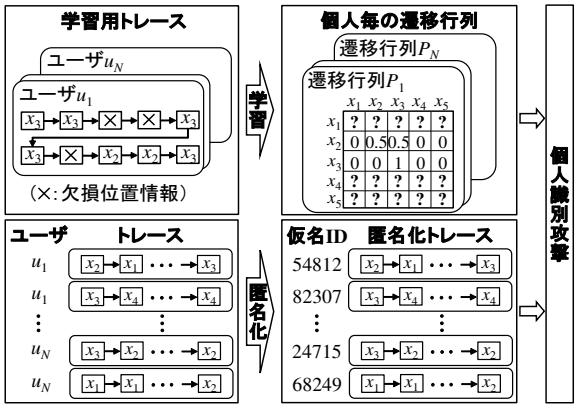

図 1: 個人識別攻撃のフレームワーク

2 個人識別攻撃

本章ではまず，Shokri らによる位置情報プライバシーのフレームワーク [9] に基づいて，個人識別攻撃のフレームワークを明確にする（第 2.1 節）．次に，ベイズ決定則に基づく個人識別攻撃 [13] を定式化する（第 2.2 節）．

2.1 個人識別攻撃のフレームワーク

本稿で考える個人識別攻撃のフレームワークを図 1 に示す（この図では学習データ不足の問題も同時に示しており，第 3 章で詳述する）．

本稿ではまず，匿名化トレースを入手できる人は，誰でも攻撃者となり得るものと仮定する（但し，トレースを第三者提供，或いは公開する事業者は除く）．例えば，トレースを第三者提供する場合は提供先の人々が，公開する場合は不特定多数の人々が攻撃者となり得る．攻撃者は，各ユーザ $u_n \in \mathcal{U}$ に対して，予め入手した（個人と紐付いた）学習用トレースを用いて遷移行列 P_n を学習する（学習用トレースの入手方法については，第 3 章で詳述する）．

次に，トレースを第三者提供（或いは公開）する事業者が，氏名などの直接識別子を削除し，（例えばランダムに生成された）仮名 ID を付与することでトレースを匿名化する．ここで本稿では簡単のため，文献 [6–9] と同様に，この匿名化トレースは全て，攻撃対象のユーザ $u_1, \cdots, u_N$ のいずれかのものであると仮定する．また，同一ユーザによる仮名 ID の異なる匿名化トレースが複数存在しても良いものとする（例えば図 1 では，ユーザ u_1 の 1 番目と 2 番目の匿名化トレースに，それぞれ仮名 ID「54812」と「82307」が割り当てられている）[2]．攻撃者は，学習した個人毎の遷移行列 $\{P_n | n \in [N]\}$ を用いて，各匿名化トレースが（ユーザ $u_1, \cdots, u_N$ のうちの）誰のものかを識別する．

尚，Shokri ら [9] は，トレースの匿名化だけでなく，（ノイズを加える，複数の領域を統合するなどの）位置情報の曖昧化（Obfuscation）も考慮している．しかし，本稿では簡単のため，位置情報の曖昧化は考えないものとする．

2.2 ベイズ決定則に基づく個人識別攻撃

本稿では，個人毎の遷移行列 $\{P_n | n \in [N]\}$ を用いた個人識別攻撃として，文献 [13] 同様，ベイズ決定則 [15] に基づく個人識別攻撃を考える [3]．ベイズ決定則は，多クラス判別において事後確率の最も大きなクラスを識別結果とする手法であり，事後確率が正しく求まるという仮定の下で，識別誤り率を最小化できることが理論的に保証される [15]．

攻撃者が時刻 1 から T までの匿名化トレースを入手したとする．この匿名化トレースの時刻 t（$1 \le t \le T$）における領域を $o_t \in \mathcal{X}$ とし，この匿名化トレースがユーザ u_n のものであるという仮説を H_n（$1 \le n \le N$）とする．このとき，匿名化トレース $o_1, \cdots, o_T$ を観測後の仮説 H_n の事後確率は，ベイズの定理より，

$$P(H_n | o_1, \cdots, o_T) = \frac{P(o_1, \cdots, o_T | H_n) P(H_n)}{\sum_{n'=1}^{N} P(o_1, \cdots, o_T | H_{n'}) P(H_{n'})} \quad (1)$$

と表せる．但し，$P(H_n)$ は仮説 H_n の事前確率であり，予め定めておく．例えば，ユーザ u_n が LBS を利用する頻度に比例するように定める方法や，簡単のため $P(H_n) = 1/N$ と一様にする

[2] これは例えば，LBS プロバイダーなどの事業者が，トレースを収集する際に氏名などの直接識別子は収集せず（即ち，最初から匿名化トレースを収集し），かつ同一ユーザが LBS を異なる日に，或いは異なる端末から利用する可能性があるためである．また，事業者が個人識別リスクの低減のため，同一ユーザの長いトレースを，仮名 ID の異なる複数のトレースに分割することも考えられる．

[3] 尚，Shokri ら [9] は，匿名化トレースが 1 ユーザあたり 1 個ずつ得られるという状況を考えている（計 $N!$ 通りのユーザとトレースの対応を考えている）．しかし，本稿では 1 ユーザあたり複数の匿名化トレースが存在し得ると仮定しているので，各匿名化トレースを「独立に」識別する攻撃を定式化する．

方法が考えられる．$P(o_1,\cdots,o_T|H_n)$ は尤度であり，遷移行列 P_n を用いて，

$$\begin{aligned} & P(o_1,\cdots,o_T|H_n) \\ =\ & P(o_1|H_n)\prod_{t=2}^{T}P(o_t|o_{t-1},H_n) \quad (2) \\ =\ & \pi_{n,o_1}\prod_{t=2}^{T}p_{n,o_{t-1},o_t}, \quad (3) \end{aligned}$$

と表せる．π_{n,o_1} は，ユーザ u_n が領域 o_1 にいるという事前確率であり，例えば遷移行列 P_n から求まる定常確率を，事前確率 $\{\pi_{n,i}|i\in[M]\}$ として用いる方法がある．

ベイズ決定則に基づく個人識別攻撃では，式(1)(3)を用いて事後確率 $P(H_n|o_1,\cdots,o_T)$ $(1\leq n\leq N)$ を算出し，その最大値を実現した仮説 H_n に対応するユーザ u_n を識別結果とする．そのようにすることで，事後確率 $P(H_n|o_1,\cdots,o_T)$ $(1\leq n\leq N)$ が正しく求まるという仮定の下，識別誤り率が最小化される．尚，この攻撃は，事後確率 $P(H_n|o_1,\cdots,o_T)$ の最も大きな上位 L 人（$1\leq L\leq N$）のユーザを識別結果とすることで，N 人のユーザから L 人の候補者に絞り込む攻撃に拡張できる．この場合は，L 人の候補者に正解が含まれない誤り率が最小化される．

3 関連文献

マルコフモデルに基づく個人識別攻撃が研究されている [6–9]．文献 [6,7] は，大量の学習用トレースを用いて（文献 [6] では約1ヶ月分，[7] では2年分以上），この手法が約 50% 以上の高い精度で個人を識別できることを示している．

しかしながら，攻撃者は学習用トレースを個人と紐付いた形で入手しなければならないことに注意が必要である．そのようなトレースとして，例えば個人が SNS（location check-in，tagging など）で公開している位置情報がある．しかし，個人が普段から公開している位置情報は一般には多くなく，また一定時間おきに公開するとも限らない．別の方法として，攻撃対象のユーザの行動を実際に観測することで，学習用トレースを入手することも考えられる．しかし，そのユーザと知人でなければ，それも一般には困難と言える．従って，学習用トレースは現実には少量で，かつ一部の位置情報が欠損し得る．文献 [6–9] では，各個人の遷移行列 P_n を独立に学習しているが，この場合に遷移行列が正しく学習できない恐れがある．

例えば，文献 [6–8] では最尤推定を用いて遷移行列 P_n を学習している．この場合における学習データ不足の問題を図1に示す．この例では，ユーザ u_1 の遷移行列 P_1 の学習に使用できるデータは，10 個の位置情報からなるトレース1つのみである．また，10 個の位置情報のうち3個は欠損している．このトレースからは領域 x_1，x_4，x_5 から次の領域への遷移が観測されないため，これを基に最尤推定を行うと，遷移確率 $p_{1,1,j}$，$p_{1,4,j}$，$p_{1,5,j}$ $(1\leq j\leq M)$ が不明となる（図1の “?”）．それ以外の要素も 0，0.5，1 といった値が入っており，明らかに過学習を引き起こしている．

文献 [9] では，学習用トレースのうち一部の位置情報が欠損している場合を考慮し，Gibbs サンプリングを用いた学習法を提案している．具体的には，ベクトル $\mathbf{p}_{n,i}=(p_{n,i,1},\cdots,p_{n,i,M})$ がディリクレ事前分布に従うと仮定し，遷移行列 P_n とユーザ u_n の欠損位置を交互にサンプリングすることを（収束するまで）繰り返した後，サンプリングされた遷移行列 P_n の平均をとることで，P_n を学習している．

しかし，この学習法も最尤推定と同様に，各個人の遷移行列 P_n を独立に学習しているため，学習データ不足の問題を抱えている．具体的には，ユーザ u_n の学習用トレースが少量の場合，たとえ欠損位置情報が正しく推定できたとしても，遷移行列 P_n の学習に使用できるデータが不足する（例えば図1で，3個の欠損位置情報を正しく推定できたとしても，遷移行列 P_1 の学習に使用できるのは 10 個の位置情報のみである）．また，ユーザ u_n の欠損位置は遷移行列 P_n を基にサンプリングするため，ユーザ u_n の学習用トレースが少量の場合，(P_n の推定精度が悪いために）欠損位置情報の推定精度も悪くなると考えられる．第6章の評価実験で，学習用トレースが少量の場合，この学習法は最尤推定と同程度の精度しか実現できないことを示す．

4 テンソル分解を用いた個人毎の遷移行列の学習

筆者らは，学習用トレースが少量の場合でも個人毎の遷移行列 $\{P_n|n\in[N]\}$ を頑健に学習するため，テンソル分解を用いた遷移行列の学習法を提案している [12, 13]．テンソルはベク

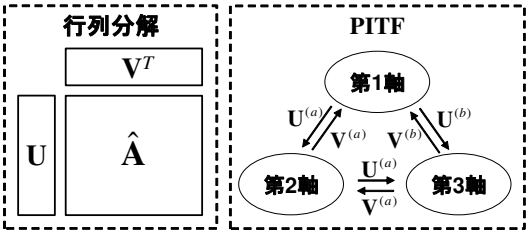

図 2: 行列分解と PITF

トルを 1 次元テンソル，行列を 2 次元テンソルとして含む多次元配列として表現できるもので [10]，テンソル分解は行列分解（Matrix Factorization）[16] を 3 次元テンソルに一般化したものである．

本章では，行列分解，テンソル分解，文献 [12, 13] の学習法について，それぞれ第 4.1 節，第 4.2 節，第 4.3 節で簡単に説明する．

4.1 行列分解

行列分解は情報推薦などで広く用いられている手法であり [16]，大きな行列を 2 つの低ランクな因子行列の積に分解して近似する（これは「低ランク近似」と呼ばれる）．これにより，少量の学習データから，行列を（未観測な要素も含めて）効率的に学習することが可能となる．

例として，行列 $\mathbf{A} \in \mathbb{R}^{N\times M}$ を分解することを考える．行列分解では，2 つの因子行列 $\mathbf{U} \in \mathbb{R}^{N\times K}$，$\mathbf{V} \in \mathbb{R}^{M\times K}$（通常，$K \ll N, M$）を用いて，行列 $\mathbf{A}$ を $\hat{\mathbf{A}} = \mathbf{U}\mathbf{V}^T$（$\hat{\mathbf{A}}$ は $\mathbf{A}$ の近似値）と分解する（図 2 左側）．行列 $\mathbf{A}$，$\hat{\mathbf{A}}$ の第 (n, i) 要素をそれぞれ $a_{n,i} \in \mathbb{R}$，$\hat{a}_{n,i} \in \mathbb{R}$ とし，行列 $\mathbf{U}$ の第 n 行を $\mathbf{u}_n \in \mathbb{R}^K$，行列 $\mathbf{V}$ の第 i 行を $\mathbf{v}_i \in \mathbb{R}^K$ とする（$1 \le n \le N$，$1 \le i \le M$）．このとき，$\hat{a}_{n,i}$ は，

$$\hat{a}_{n,i} = \langle \mathbf{u}_n, \mathbf{v}_i \rangle \tag{4}$$

と表せる．$\mathbf{u}_n$，$\mathbf{v}_i$ は因子ベクトルと呼ばれ，通常，正規化二乗誤差を最小化するように学習される [16]（学習アルゴリズムは割愛する）．

このように行列 $\mathbf{A}$ に低ランク性を仮定することで，推定すべき行列要素数は大幅に削減される（即ち，次元圧縮）．その結果，少量の学習データを基に，行列 $\mathbf{A}$ を（未観測な要素も含めて）効率的に学習することが可能となる．

4.2 テンソル分解

テンソル分解は，行列分解を 3 次元テンソルに一般化したものである．3 次元テンソルの分解方法としては様々なものがあり，Tucker 分解 [10] や CP 分解 [10] が代表的であるが，本稿では PITF（Pairwise Interaction Tensor Factorization）[11] に着眼する．PITF は Tucker 分解や CP 分解よりも簡潔なモデルであり，より良い性能が実現できることも示されている [11]．

以下，PITF を詳述する．ここでは説明の都合上，例として $N \times M \times M$ の 3 次元テンソル $\mathcal{A} \in \mathbb{R}^{N\times M\times M}$ を考える．テンソル $\mathcal{A}$ の第 (n, i, j) 番目の要素を $a_{n,i,j} \in \mathbb{R}$ とする．PITF は，$a_{n,i,j}$ を以下のように近似する．

$$\hat{a}_{n,i,j} = \langle \mathbf{u}_n^{(a)}, \mathbf{v}_i^{(a)} \rangle + \langle \mathbf{u}_n^{(b)}, \mathbf{v}_j^{(b)} \rangle + \langle \mathbf{u}_i^{(c)}, \mathbf{v}_j^{(c)} \rangle \tag{5}$$

但し，$\hat{a}_{n,i,j}$ は $a_{n,i,j}$ の近似値であり，$\mathbf{u}_n^{(a)}, \mathbf{v}_i^{(a)}$, $\mathbf{u}_n^{(b)}, \mathbf{v}_j^{(b)}, \mathbf{u}_i^{(c)}, \mathbf{v}_j^{(c)} \in \mathbb{R}^K$ は因子ベクトルである．これらに対応する因子行列を，それぞれ $\mathbf{U}^{(a)} \in \mathbb{R}^{N\times K}$，$\mathbf{V}^{(a)} \in \mathbb{R}^{M\times K}$，$\mathbf{U}^{(b)} \in \mathbb{R}^{N\times K}$，$\mathbf{V}^{(b)} \in \mathbb{R}^{M\times K}$，$\mathbf{U}^{(c)} \in \mathbb{R}^{M\times K}$，$\mathbf{V}^{(c)} \in \mathbb{R}^{M\times K}$ とする（例えば $\mathbf{u}_n^{(a)}$ は $\mathbf{U}^{(a)}$ の第 n 行）．このとき，式 (4)(5) より，PITF は第 1 軸と第 2 軸の相互作用を $\mathbf{U}^{(a)}\mathbf{V}^{(a)T}$，第 1 軸と第 3 軸の相互作用を $\mathbf{U}^{(b)}\mathbf{V}^{(b)T}$，第 2 軸と第 3 軸の相互作用を $\mathbf{U}^{(c)}\mathbf{V}^{(c)T}$ とモデル化する，という意味で行列分解の一般化になっている（図 2 右側）．

4.3 遷移確率テンソルの学習

個人毎の遷移行列の集合は，ユーザ（User），領域（From Region），次の時刻における領域（To Region）の 3 軸で構成される 3 次元テンソルと見なすことができる．本稿では，これを「遷移確率テンソル」と呼ぶ．しかし，このテンソルは To Region に対する和が常に 1 となっており（即ち，$\sum_j p_{n,i,j} = 1$），この制約の下で分解して学習するのは困難である．

そこで，筆者らは遷移確率テンソルではなく，学習データから各遷移の回数を数えることで求めた「遷移回数テンソル」を分解して各要素を学習した後，To Region に対する和が 1 となるように正規化することで遷移確率テンソルを求める学習法を提案している [12,13]（図 3）．具体的には，遷移回数テンソルを第 4.2 節のテン

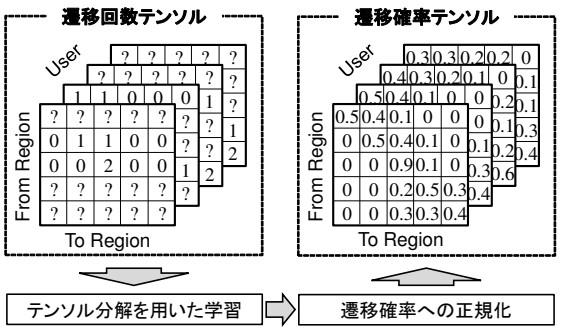

図 3: テンソル分解を用いた遷移確率テンソルの学習法 [12,13]（“?” は To Region に渡って遷移回数が全て 0 となっている要素）

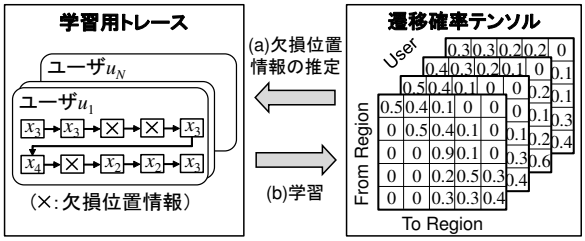

図 4: 欠損位置情報の推定を伴う遷移確率テンソルの学習法

ソル $\mathcal{A}$ に当てはめ，遷移回数が非負値であるという制約の下で,（To Region に渡って遷移回数が全て 0 となっている要素は除いて）正規化二乗誤差を最小化するようにパラメータ $\Theta = \{\mathbf{U}^{(a)}, \mathbf{V}^{(a)}, \mathbf{U}^{(b)}, \mathbf{V}^{(b)}, \mathbf{U}^{(c)}, \mathbf{V}^{(c)}\}$ を学習している（学習アルゴリズムは割愛する）．

この学習法の，最尤推定 [6–8] や Gibbs サンプリングを用いた学習法 [9] との最大の違いは，各個人の遷移行列を独立に学習するのではなく，遷移確率テンソルに対して低ランク性を仮定して，その全体を学習する点にある．そうすることで,「全ユーザの学習データ」を基に，各個人の遷移行列が互いに影響を及ぼし合うように，遷移確率テンソルを（未観測な要素も含めて）効率的に学習することが可能となる．

5　欠損位置情報の推定を伴う学習

学習用トレースには，一部の位置情報が欠損し得る．この欠損位置情報を正しく推定できれば，使用できる学習データが増えるため，遷移確率テンソル（即ち，個人毎の遷移行列）の推定精度も上がると考えられる．

そこで，本稿では (a) 学習した遷移確率テンソルを用いて欠損位置情報を Viterbi アルゴリズム [14] により推定し，(b) 推定した欠損位置情報を基に遷移確率テンソル（パラメータ Θ）を学習し直すことを，交互に繰り返す学習法を提案する（図 4 参照）．このように欠損データの推定とパラメータの推定を交互に繰り返す考え方は，EM（Expectation Maximization）アルゴリズム [17] に基づいている．EM アルゴリズムは繰り返しの度に尤度が単調に増加するため，欠損位置情報とパラメータ Θ の推定を繰り返すことによって，欠損位置情報と遷移確率テンソルの推定精度も上がっていくと考えられる．

尚，Gibbs サンプリングを用いた学習法 [9] も遷移行列 P_n と欠損位置のサンプリングを交互に繰り返すが，この手法は（第 3 章でも述べたように）各個人の遷移行列 P_n を独立に学習する．一方，提案手法では，各個人の遷移行列が互いに影響を及ぼし合うように遷移確率テンソルを学習するため,「全ユーザの学習データ」を基に，尤もらしい欠損位置情報と遷移確率テンソルを推定することが可能となる．

以下，欠損位置情報の推定方法を説明する．ここでは，$T'(< T)$ 個の欠損位置を含むトレース $z_{n,1}, \cdots, z_{n,T}$ が学習データとして与えられるものとする．但し，$z_{n,t}$ は時刻 t における位置が欠損していなければ $z_{n,t} \in \{x_1, \cdots, x_M\}$（実際の領域），欠損していれば $z_{n,t} = \perp$（$\perp$ は欠損位置を表す記号）をとる（即ち，$z_{n,t} \in \mathcal{X} \cup \{\perp\}$ であり，$z_{n,1}, \cdots, z_{n,T}$ のうち T' 個は $\perp$ である）．

T' 個の欠損位置を含む学習用トレース $z_{n,1}, \cdots, z_{n,T}$ が与えられたとき,（欠損位置の推定値を含めて）最も事後確率の大きいトレース $X_{n,1}, \cdots, X_{n,T}$（但し，$X_{n,t} \in \mathcal{X}$ はユーザ u_n の時刻 t における領域を表す確率変数）を推定することを考える．これは,

$$\underset{X_{n,1},\cdots,X_{n,T}}{\arg\max} \ \Pr(X_{n,1}, \cdots, X_{n,T} | z_{n,1}, \cdots, z_{n,T}) \quad (6)$$

と表せる．トレース $X_{n,1}, \cdots, X_{n,T}$ の候補数は $M^{T'}$ 個あり，欠損位置の数 T' に対して指数関数的に増加するため，式 (6) の厳密な計算は時間がかかる．

従って本稿では，Viterbi アルゴリズム [14] を用いて欠損位置を推定する．Viterbi アルゴ

リズム [14] の詳細は，紙面の都合上省略するが（詳細は文献 [14] を参照），式 (6) の近似解を欠損位置の数 T' に対して $O(T')$ の計算量で求めるアルゴリズムである．

提案手法を纏めると，以下のとおりである．

1. 遷移確率テンソル（パラメータ Θ）を学習する（第 4.3 節参照）．
2. Viterbi アルゴリズム [14] を用いて，式 (6) の最大値を近似するトレース $X_{n,1}, \cdots, X_{n,T}$ を求める（T' 個の欠損位置の推定値は，そのトレースの中に含まれている）．
3. 遷移回数を数え直し，遷移確率テンソル（パラメータ Θ）を再学習する（第 4.3 節参照）．
4. ステップ 2. と 3. を一定回数繰り返す．

このように遷移確率テンソルを再学習することで，個人識別攻撃の精度が飛躍的に向上することを第 6 章で示す．

6 評価実験

6.1 実験条件

提案手法の有効性を検証するため，Geolife データセット [18] を用いた評価実験を行った．このデータセットは，Microsoft Research Asia が 182 名の被験者のトレースを，2007 年から 2012 年にかけて収集したものである（通勤，買い物，旅行など様々な活動のトレースを含んでいる）．ほとんどのトレースは北京にあったため，本実験では北京のトレースのみを用いた．

各被験者に対して，30 分以上の時間間隔で位置情報を取り出し，10 個の位置情報（$T = 10$）からなるトレースを 10 個取り出した．但し，そのようなトレースが 10 個も取り出せない被験者が 102 名いたため，残りの 80 名の被験者（$N = 80$）のトレースを実験に用いた．また，全トレースを含む領域を，均等に縦 16 個 ×横 16 個の領域（$M = 256$）に分割した．

各被験者に対して，10 トレースのうち 2 つを学習用に，残りの 8 つを評価用に用いた．このときの学習用トレースの選び方としては，${}_{10}C_2 = 45$ 通りを全て試し，その各々の場合に対して，各学習用トレースからランダムに T'（$0 \leq T' < 10$）個の位置を欠損位置として選び，削除した．この学習用トレースから個人毎の遷移行列 $\{P_n | n \in [N]\}$ を学習した．

学習法としては，最尤推定 [6–8]（「**ML**」と表記，第 3 章参照），Gibbs サンプリングを用いた学習法 [9]（「**GS**」と表記，第 3 章参照），テンソル分解を用いた学習法 [12, 13]（「**TF**」と表記，第 4.3 節参照），提案手法（「**TF-V**」と表記，第 5 章参照）の 4 つを比較した．

ML と **GS** では，遷移確率 $p_{n,i,j}$ が不明な場合には $p_{n,i,j} = 1/M$ と一様に設定した．また，$p_{n,i,j} = 0$ となる場合には，文献 [6] 同様，非常に小さな値（$p_{n,i,j} = 10^{-16}$）を代入した（これは，式 (3) によって算出される尤度 $P(o_1, \cdots, o_T | H_n)$ が 0 となるのを回避するためである）．**TF** と **TF-V** では，テンソルの分解方法として PITF（第 4.2 章参照）を用い，因子ベクトルの次元数としては $K = 16$ とした（$K = 8, 16, 32, 64$ と試したが，16 と 32 のときに最も高い精度を実現していた）．**TF-V** では，欠損位置の推定と遷移確率テンソルの再学習の繰り返し回数は 1 回とした（1, 3, 5 回と試したが，1 回で 5 回の場合とほぼ同程度の精度を実現していた）．

学習された遷移行列 $\{P_n | n \in [N]\}$ を用いて，計 $45 \times 8 = 360$ 個の評価用トレースの各々に対して，ベイズ決定則に基づく個人識別攻撃（第 2.2 節参照）を実行した．その際，式 (1) における事前確率 $P(H_n)$ は，$P(H_n) = 1/N$ と一様に設定し，式 (3) における事前確率 $\pi_{n,i}$ については，P_n から算出される定常確率を用いた．このときの候補者数 L と攻撃成功割合（L 個の候補者の中に正解が含まれていた割合）を評価した．

6.2 実験結果

候補者数を $L = 1$ 或いは $L = 10$ としたときの，欠損位置数 $T'(\in \{0, 2, 4, 6, 8\})$ と攻撃成功割合の関係を図 5 に示す．また，1 被験者の学習用トレースにおける，欠損していない位置同士の遷移数の平均を表 1 に示す（例えば $T' = 0$ であれば，$2 \times (10 - 1) = 18$ 個）．

図 5 より，**GS**（Gibbs サンプリングを用いた学習法 [9]）が **ML**（最尤推定 [6–8]）と同程度の精度しか実現できていないことが分かる．これは，（第 3 章で述べたように）**GS** は各個人の遷移行列 P_n を独立に学習しており，P_n の推定精度，及び P_n を基にした欠損位置の推定精度が悪いためと考える．また，**TF**（テンソル分解を用いた学習法 [12, 13]）は，$T' = 0, 2, 4$ のと

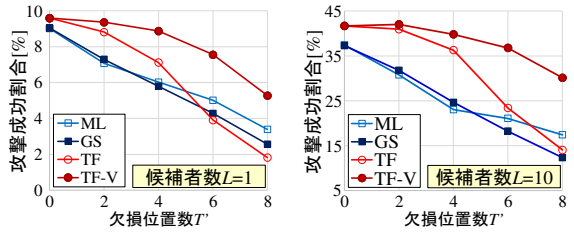

図 5: 欠損位置数 T' と攻撃成功割合の関係

表 1: 1 被験者の学習用トレースにおける，欠損していない位置同士の遷移数の平均

T'	0	2	4	6	8
遷移数の平均	18	11.5	6.43	2.84	0.69

きは **ML** や **GS** よりも精度が高いが，$T' = 6, 8$ のときは同程度の精度しか得られていない．これは，$T' = 6, 8$ のときは欠損していない位置同士の遷移数（即ち，学習データ量）があまりにも少なかったためと考える（1 被験者あたりの平均は，表 1 よりそれぞれ 2.84，0.69 である）．

一方，**TF-V**（提案手法）ではこれら 3 つの学習法を大幅に上回る精度を実現している．これは，(第 5 章で述べたように）提案手法では「全ユーザの学習データ」を基に，各個人の遷移行列が互いに影響を及ぼし合いながら，尤もらしい欠損位置情報と遷移確率テンソルを推定することができたためと考えている．$T' = 6, 8$ のときでも高い精度を実現しているのは，欠損位置を正しく推定することで，実質的に学習データ量を大幅に増やすことに成功したためである．

例えば，$T' = 6$ のときの攻撃成功確率は，**ML** では 5.0%（$L = 1$），21%（$L = 10$），**GS** では 4.3%（$L = 1$），18%（$L = 10$）なのに対して，**TF-V** では 7.5%（$L = 1$），37%（$L = 10$）である．以上より，提案手法の有効性が示された．

7 まとめ

本稿では欠損位置情報の推定と，テンソル分解による個人毎の遷移行列の学習を繰り返す学習法を提案し，個人識別攻撃に適用して有効性を示した．この成果は，学習用トレースが少量で，かつ一部の位置情報が欠損するという現実的な状況での個人識別攻撃を考える上で大きな役割を果たすものと考えている．

今後は，匿名化と位置情報の曖昧化の両方が施された場合の評価実験などを検討している．

謝辞 本研究は JSPS 科研費 26880030 の助成を受けたものである．また，産総研の兼村厚範氏，赤穂昭太郎氏，筑波大の日野英逸氏より有益な技術的コメントを頂いたので感謝する．

参考文献

[1] S. Shekhar *et al.*, “Spatial big-data challenges intersecting mobility and cloud computing,” Proc. ACM MobiDE’12, pp.1–12, 2012.
[2] Y. Zheng *et al.*, “Mining interesting locations and travel sequences from GPS trajectories,” Proc. WWW’09, pp.791–800, 2009.
[3] B. Hull *et al.*, “CarTel: A distributed mobile sensor computing system,” Proc. SenSys’06, pp.125–138, 2006.
[4] J. Freudiger, R. Shokri, and J.-P. Hubaux, “Evaluating the privacy risk of location-based services,” Proc. FC’11, pp.31–46, 2011.
[5] M. Srivatsa and M. Hicks, “Deanonymizing mobility traces: Using social networks as a side-channel,” Proc. ACM CCS’12, pp.628–637, 2012.
[6] Y. D. Mulder *et al.*, “Identification via location-profiling in GSM networks,” Proc. ACM WPES’08, pp.23–32, 2008.
[7] S. Gambs *et al.*, “De-anonymization attack on geolocated data,” Proc. IEEE TrustCom’13, pp.789–797, 2013.
[8] R. Shokri *et al.*, “Quantifying location privacy: The case of sporadic location exposure,” Proc. PETS’11, pp.57–76, 2011.
[9] R. Shokri *et al.*, “Quantifying location privacy,” Proc. IEEE S&P’11, pp.247–262, 2011.
[10] T. G. Kolda and B. W. Bader, “Tensor decompositions and applications,” SIAM Review, vol.51, no.3, pp.455–500, 2009.
[11] S. Rendle and L. Shmidt-Thieme, “Pairwise interaction tensor factorization for personalized tag recommendation,” Proc. ACM WSDM’10, pp.81–90, 2010.
[12] T. Murakami and H. Watanabe, “Location prediction attacks using tensor factorization and optimal defenses,” Proc. IEEE BDSP’14, pp.13–21, 2014.
[13] T. Murakami, A. Kanemura, and H. Hino, “Group sparsity tensor factorization for de-anonymization of mobility traces,” Proc. IEEE TrustCom’15, 2015 (to appear).
[14] L. R. Rabiner, “A tutorial on hidden markov models and selected applications in speech recognition,” Proc. IEEE, vol.77, no.2, pp.257–286, 1989.
[15] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification. Wiley-Interscience, 2000.
[16] Y. Koren, R. Bell, and C. Volinsky, “Matrix factorization techniques for recommender systems,” IEEE Computer, vol.42, no.8, pp.30–37, 2009.
[17] J. L. Schafer and M. K. Olsen, “Multiple imputation for multivariate missing-data problems: A data analyst’s perspective,” Multivariate Behavioral Research, vol.33, no.4, pp.545–571, 1998.
[18] Y. Zheng, X. Xie, and W.-Y. Ma, “GeoLife: A collaborative social networking service among user, location and trajectory,” IEEE Data Engineering Bulletin, vol.32, no.2, pp.32–40, 2010.