Vol.2013-DBS-157 No.1
Vol.2013-IFAT-111 No.1
2013/7/22

マルコフ過程を用いた 位置情報継続開示のためのアドバーザリアルプライバシ

川本 淳平[1,a)]　佐久間 淳[2]

概要：本論文では，位置情報を継続的に公開するためのプライバシ定義を提案する．ある時刻における人々の位置情報は，過去に滞在していた地点との相関がある．そのため，差分プライバシのようにどのような背景知識を持つ攻撃者に対して，安全かつ継続的に位置情報を公開するためには付加しなければならないノイズ量が多くなる．本論文では，人々の行動にマルコフ性を仮定しマルコフ過程を用いた攻撃者に対して安全な位置情報の公開のためのアドバーザリアルプライバシを提案する．本論文では，先ず，各時刻毎に POI 別滞在人数ヒストグラムを公開する問題を考え，提案アドバーザリアルプライバシを満足するヒストグラム導出メカニズムについて議論する．そして，各時刻毎に POI のシーケンスからなるパスのカウントヒストグラムを公開する問題を考え，先のヒストグラム導出メカニズムをこの問題へ拡張する．最後に評価実験では，公開位置情報を用いた解析タスクとして頻出パス抽出を想定し，提案手法がプライバシを保護しつつ正確な解析結果を導く位置情報を公開できることを示す．

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より，それらに搭載されている GPS から大人数の位置情報をリアルタイムに収集することが可能になった．この大規模な位置情報群は，事故や渋滞の早期発見や自然災害発生時における人の流れなど様々な解析に利用が期待されている．特に，これらの位置情報を用いることで，人手による解析よりも迅速な解析や，人手をあまりかけることのできない過疎地域における解析への利用が期待できる．

GPS から得られた人々の位置情報を解析のために公開することを考えると，公開する位置情報に対するプライバシ保護が必要となる．なぜなら，多くの場合，位置情報はプライベートな情報だからである．位置情報のためのプライバシ保護データ出版に関する研究はいくつか行われており，代表的なものとして差分プライバシ [1] を用いる手法がある [2], [3]．差分プライバシは，どのような背景知識を持つ攻撃者に対してもプライベート性を保証するプライバシ定義であり，出力は演算結果にラプラスノイズなど摂動を付加することで行われる．一方，差分プライバシの問題点はあらゆる背景知識を持つ攻撃者にたいしてプライベートであることを保障するため，付加するノイズ量が多いことである．特に，パス長が長くスパース性が現れるとノイズの影響が無視できない．[2], [3] では，出力結果を頻出パス解析に用いると解析目標を限定し，稀なパスを予め削除することと，考えるパスの最大長を制限することによりスパース性の問題に取り組んでいる．我々の目標は，位置情報を過疎地域における解析にも用いることであり，稀なパスを削除するという手法は利用しがたい．

これらの既存手法は，データベースや演算結果の一度きりの出版を前提としており，時間が経過した後再び更新した情報を出版することは考慮されていない．一般に，複数回公開する場合，過去に出版した情報を用いた攻撃も考慮する必要がある．特に位置情報においては，時間的空間的制約により，ある時点に人々が滞在できる範囲は過去の位置情報に強く依存する．例えば，短時間の間に東京とニューヨークの両方を訪れることは不可能であり，また，局所的であっても河川や山などにより移動が困難である場合が考えられる．攻撃者はこうした地理的制約を用いた攻撃を行えると想定すべきであり，したがって過去に出版した情報を考慮した出版が必要となる．

差分プライバシは攻撃者の背景知識を仮定せず任意の背景知識を持つ攻撃者に対してプライベートな情報を出力する．そのため，過去に出力した値と相関のある位置情報の継続的公開ではノイズが大きくなってしまう．一方で，あらゆる背景知識を用いた攻撃に対してプライベートである必要が無い場合もある．例えば，ほとんどの人が直進する交差点があり，そのことは攻撃者を含め一般的に知れ渡っ

[1] 筑波大学システム情報系, 茨城県つくば市天王台 1-1-1
[2] 筑波大学大学院システム情報工学研究科
[a)] junpei@mdl.cs.tsukuba.ac.jp

ている情報であるとする．差分プライバシではこの交差点で直進したのか右左折したのかまでプライベートにするが，我々は，直進ではなく右左折した場合のみプライバシを考慮すれば良いと考える．言い換えれば，攻撃者を含め一般的に知られている行動に関してはプライバシを考慮しない代わりより正確な情報を公開することを考える．

本論文では，人々の行動が一般的に知られている行動であるか否かをマルコフ過程を用いて表現する．そして，どのような情報をプライベートにすべきかを定義するために，攻撃者に関する仮定を置き，その攻撃者のクラスに対する安全性を定義する．そのために，本論文ではアドバーザリアルプライバシ [4] を採用する．アドバーザリアルプライバシでは，攻撃者はある推測を行うものとして定義され，その推測確信度が出力情報を観測した前後であまり変化しないとき，その出力情報はプライベートであるという．

本論文では，各時刻毎に POI 別滞在人数ヒストグラムを公開する問題を考え，提案アドバーザリアルプライバシを満足するヒストグラム導出メカニズムについて議論する．我々の提案プライバシは，稀な行動であってもマルコフ過程から自明な遷移である場合はプライバシをあまり考慮しない．そのため，交差点が少ないなど行動の種類がそれほど多くない過疎地域において，多くの場合に差分プライバシに比べて正確な位置情報を出力することができる．評価実験では，公開位置情報を用いた解析タスクとして頻出パス抽出を想定し，提案手法がプライバシを保護しつつ正確な解析結果を導く位置情報を公開できることを示す．

2. 基本事項

本論文では，位置情報を集約し公開する集約者，N 人の位置情報を提供する人々 $U = \{u_1, u_2, \cdots, u_N\}$，そして公開された位置情報から人々の滞在位置を取得しようとする攻撃者を考える．本節では，集約者及び人々とその行動ついて定義する．攻撃者については，改めて 3 節で議論する．

集約者は，ある時間間隔 Δt で人々の端末から緯度・経度情報を受け取ると，それら緯度・経度情報を解析の目的に合わせて予め与えられている POI に対応付ける．そして，各時刻ごとに各 POI における滞在人数の分布，すなわちヒストグラムを出力する．また，ヒストグラムの公開間隔 Δt も同様に与えられるとする．

今，L 個の POI $\{\ell_1, \ell_2, \cdots, \ell_L\}$ が与えられているとすると，時刻 t におけるヒストグラムは L 次元のベクトル $\boldsymbol{\pi}(t)$ と書く．すなわち，$\boldsymbol{\pi}(t)$ の i 番目の要素を $\pi_i(t)$ と書くと，これは時刻 t において POI ℓ_i に滞在している人数を表す．我々は，与えられた POI をその実際の位置関係を *POI* **グラフ** として表現する．この グラフにおける頂点集合 V_{POI} は POI 集合に等しく $V_{\mathrm{POI}} = \{\ell_1, \ell_2, \cdots, \ell_L\}$ である．また，ヒストグラムの公開間隔 Δt で到達可能な POI 間に無向枝を張り，その枝集合を E_{POI} と書く．このとき POI グラフ G_{POI} は $G_{\mathrm{POI}} = (V_{\mathrm{POI}}, E_{\mathrm{POI}})$ となる．

本論文では，人々の行動を確率モデルを用いて扱う．[3] で議論されているように，人々の行動はマルコフ過程 [5] を用いて表現できる．マルコフ過程は，状態集合 S と遷移確率行列 $\boldsymbol{P}$ によって定まり，$M(S, \boldsymbol{P})$ と書く．なお，行列 $\boldsymbol{P}$ の (i, j) 成分を $P_{i,j}$ と書く．一般的に n 階マルコフ過程は状態集合の置き換えにより 1 階マルコフ過程（以降，マルコフ過程と書く）として表現できる．そこで，先ずはマルコフ過程を用いて議論し，高階マルコフ過程については 5 節にて議論する．状態集合 S_1 として G_{POI} における頂点，すなわち POI 集合を考える．また，遷移確率行列 $\boldsymbol{P}_1$ は，ヒストグラムの公開間隔 Δt によって定まり，与えられるものとする．

3. プライバシ定義

差分プライバシ [1] は，攻撃者の背景知識を仮定せず任意の背景知識を持つ攻撃者に対してプライベートな情報を出力する．そして，スパース性を持つデータや複数回出版を行う場合，付加するノイズ量が多くなることが知られている．本稿では我々が提案するのは，差分プライバシの攻撃者の背景知識を仮定しないという特徴を緩め，過去に公開したヒストグラムや 2 節で定義したマルコフ過程を攻撃に用いる攻撃者など，いくつかの攻撃者のクラスを仮定し，それぞれのクラスに対してプライベート性を定義し，差分プライバシを満たす出力に比べて損失の少ないヒストグラムの出版を行う．このように攻撃者を仮定するプライバシ定義はアドバーザリアルプライバシ [4] と呼ばれる．

3.1 アドバーザリアルプライバシ

アドバーザリアルプライバシ [4] では，攻撃者はある決められた推測を行う．そして，その推測確信度が出力情報を観測した前後であまり変化しないとき，その出力情報はアドバーザリアルプライベートであるという．

定義 3.1. 攻撃者が出力情報 O を観測する前の入力 X の推測の確信度を $p(X)$，出力情報を観測した後の推測の確信度を $p(X|O)$ と書くことにする．出力情報を観測した前後において攻撃者の確信度がある $\epsilon > 0$ に対して，

$$\forall X, \quad p(X|O) \leq e^{\epsilon} p(X)$$

である時，O は ϵ-アドバーザリアルプライベートという．

本論文では，ある攻撃対象 $u \in U$ の時刻 t における滞在 POI ℓ_j の推測を攻撃者の推測とする．そして，その確信度を $p(X_t^u = \ell_j)$ と書く．また，攻撃者が観測する出力情報は時刻 t におけるヒストグラム $\boldsymbol{\pi}(t)$ である．

攻撃者の推測には様々な方法が考えられる．アドバーザリアルプライバシでは，攻撃者の背景知識や推測能力に仮定を置き，そのクラスの攻撃者に対する安全性を議論する．本論文では，背景知識を K，出力ヒストグラムを観測す

る前後における推測アルゴリズムをそれぞれ f, g と書く．そして，一つの攻撃者のクラスが (K, f, g) にて定める．この時，$(K_{\mathsf{ADV}}, f_{\mathsf{ADV}}, g_{\mathsf{ADV}})$ にて定まる攻撃者 ADV に対して出力情報を観測する前後における推測はそれぞれ，

$$p(X_t^u = \ell_j) = f_{\mathsf{ADV}}(u, t, \ell_j, K_{\mathsf{ADV}}),$$
$$p(X_t^u = \ell_j | \boldsymbol{\pi}(t)) = g_{\mathsf{ADV}}(u, t, \ell_j, \boldsymbol{\pi}(t), K_{\mathsf{ADV}})$$

である．また，出力情報の観測前後における確信度比を出力情報が攻撃者の確信度に与える贈与として定義する．

定義 3.2. 攻撃者のクラス $\mathsf{ADV}(K_{\mathsf{ADV}}, f_{\mathsf{ADV}}, g_{\mathsf{ADV}})$ に対して，出力情報 $\boldsymbol{\pi}(t)$ が推測 $X_t^u = \ell_j$ に与える贈与は，

$$\mathrm{Gain}_{\mathsf{ADV}}(\boldsymbol{\pi}(t), u, t, \ell_j, K_{\mathsf{ADV}}) = \frac{g_{\mathsf{ADV}}(u, t, \ell_j, \boldsymbol{\pi}(t), K_{\mathsf{ADV}})}{f_{\mathsf{ADV}}(u, t, \ell_j, K_{\mathsf{ADV}})}.$$

よって，$\forall u, \ell_j, \mathrm{Gain}_{\mathsf{ADV}}(\boldsymbol{\pi}(t), u, t, \ell_j, K_{\mathsf{ADV}}) \leq e^\epsilon$ である時，言い換えれば，$\max_{u,\ell_j} \mathrm{Gain}_{\mathsf{ADV}}(\boldsymbol{\pi}(t), u, t, \ell_j, K_{\mathsf{ADV}}) \leq e^\epsilon$ である時，出力情報 $\boldsymbol{\pi}(t)$ は攻撃者のクラス ADV に対して ϵ-アドバーザリアルプライベートである．

3.2 攻撃者のクラス

一般的に攻撃者が攻撃に利用できる情報が少ない場合，攻撃者による推測のバリエーションが増加しプライバシ保護が難しくなることが知られている [6], [7]．アドバーザリアルプライバシにおいては，出力情報を観測する前の推測，すなわち f による予測精度が悪いと出力ヒストグラムが与える贈与が大きくなり，アドバーザリアルプライベートな出力を計算することが難しくなる．そのため，関数 f を適切に定める必要がある．また，プライバシ保護においては，攻撃者の能力とプライバシの保護しやすさの間にトレードオフがある．そこで，本論文では，ユースケース別にいくつかの攻撃者のクラスを提案する．

3.2.1 マルコフ過程を知識として持つ攻撃者

まず，マルコフ過程 $M_1(S_1, \boldsymbol{P}_1)$ 及び時刻 t までに公開されたヒストグラム $\boldsymbol{\pi}(1), \boldsymbol{\pi}(2), \cdots, \boldsymbol{\pi}(t-1)$ を推測に利用できる攻撃者のクラス $\mathsf{MK}(K_{\mathsf{MK}}, f_{\mathsf{MK}}, g_{\mathsf{MK}})$ を考える．すなわち，この攻撃者は，公開されたヒストグラムを基にある人が時刻 t にどの POI に滞在しているのかを推測する．

マルコフ性の仮定より，時刻 t までに公開されたヒストグラムのうち，時刻 t における滞在 POI の推測に影響するのは $\boldsymbol{\pi}(t-1)$ のみである．したがって，このクラスの攻撃者の背景知識は時刻 $t-1$ に公開された $\boldsymbol{\pi}(t-1)$ とマルコフ遷移確率 $\boldsymbol{P}_1$ であり，$K_{\mathsf{MK}} = \{\boldsymbol{\pi}(t-1), \boldsymbol{P}_1\}$ となる．

我々は，このクラスの攻撃者が出力ヒストグラムの観測前後において，攻撃対象 u が時刻 t に POI ℓ_j に滞在していると推測する場合の確信度 $f_{\mathsf{MK}}, g_{\mathsf{MK}}$ をそれぞれ，

$$f_{\mathsf{MK}}(u, t, \ell_j, \{\boldsymbol{\pi}(t-1), \boldsymbol{P}_1\}) = p(X_t^u = \ell_j | \tilde{\boldsymbol{\pi}}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)$$
$$= \frac{p(\tilde{\boldsymbol{\pi}}(t), \boldsymbol{\pi}(t-1) | X_t^u = \ell_j; \boldsymbol{P}_1) p(X_t^u = \ell_j; \boldsymbol{P}_1)}{p(\tilde{\boldsymbol{\pi}}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)}$$

$$g_{\mathsf{MK}}(u, t, \ell_j, \boldsymbol{\pi}(t), \{\boldsymbol{\pi}(t-1), \boldsymbol{P}_1\}) = p(X_t^u = \ell_j | \boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)$$
$$= \frac{p(\boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1) | X_t^u = \ell_j; \boldsymbol{P}_1) p(X_t^u = \ell_j; \boldsymbol{P}_1)}{p(\boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)}$$

と定める．ここで，$\tilde{\boldsymbol{\pi}}(t)$ は $\boldsymbol{\pi}(t-1)$ と遷移確率 $\boldsymbol{P}_1$ から予測されるヒストグラム $\tilde{\boldsymbol{\pi}}(t) = (\boldsymbol{\pi}(t-1)^t \boldsymbol{P}_1)^t$ である．

上記条件付き確率 $p(\boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1) | X_t^u = \ell_j; \boldsymbol{P}_1)$ は，攻撃対象 u の時刻 t における滞在 POI を固定した場合の $\boldsymbol{\pi}(t-1)$ 及び $\boldsymbol{\pi}(t)$ の実現確率である．これは，第 j 要素が 1 の単位ベクトル $\boldsymbol{e}_j$ により，$p(\boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1) | X_t^u = \ell_j; \boldsymbol{P}_1) = p(\boldsymbol{\pi}(t) - \boldsymbol{e}_j, \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)$ と書ける．

以上より，攻撃者のクラス MK の攻撃者がある攻撃対象が時刻 t に ℓ_j に滞在していると推測する場合の出力ヒストグラム $\boldsymbol{\pi}(t)$ による確信度の贈与は，

$$\mathrm{Gain}_{\mathsf{MK}}(\boldsymbol{\pi}(t), u, t, \ell_j, \{\boldsymbol{\pi}(t-1), \boldsymbol{P}_1\})$$
$$= \frac{p(\boldsymbol{\pi}(t) - \boldsymbol{e}_j, \boldsymbol{\pi}(t-1); \boldsymbol{P}_1) p(\tilde{\boldsymbol{\pi}}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)}{p(\tilde{\boldsymbol{\pi}}(t) - \boldsymbol{e}_j, \boldsymbol{\pi}(t-1); \boldsymbol{P}_1) p(\boldsymbol{\pi}(t), \boldsymbol{\pi}(t-1); \boldsymbol{P}_1)}. \quad (1)$$

式中の四つの確率は，それぞれ二つのヒストグラムの実現確率である[*1]．この実現確率を求めるために，時刻 $t-1$ から t の間の人々の行動を考える．ℓ_i から ℓ_j に移動した人数を $a_{i,j}$ と書くと，それぞれの時刻におけるヒストグラムが $\boldsymbol{\pi}(t-1)$，$\boldsymbol{\pi}(t)$ のとき，$A = \{a_{i,j} \,|\, i, j \in [1, L], \sum_{j=1}^L a_{i,j} = \pi_i(t-1), \sum_{i=1}^L a_{i,j} = \pi_j(t)\}$ は $\boldsymbol{\pi}(t-1)$，$\boldsymbol{\pi}(t)$ に矛盾しない人々の行動の一つを表す．このような人々の行動は複数存在するため，その全体を $\mathcal{A}(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t))$ と書く．この時，あるヒストグラム $\boldsymbol{\pi}(t-1)$，$\boldsymbol{\pi}(t)$ の実現確率は，

$$p(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t); \boldsymbol{P}_1) = \sum_{A \in \mathcal{A}(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t))} \prod_{i=1}^L \prod_{j=1}^L P_{i,j}^{a_{i,j}} \quad (2)$$

である．一方，二つのヒストグラムに矛盾しない人々の行動の数 $|\mathcal{A}(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t))|$ は，$N!$ 通り考えられ，式 (2) を厳密に求めることは現実的ではない．そこで，

$$N! \times \max_{A \in \mathcal{A}(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t))} \prod_{i=1}^L \prod_{j=1}^L P_{i,j}^{a_{i,j}} \quad (3)$$

を用いる．この値の効率的な計算方法は 4.1 節にて述べる．

3.2.2 時刻 t における一人分の滞在 POI を知る攻撃者

マルコフ過程 M_1 と過去に公開されたヒストグラム $\boldsymbol{\pi}(1), \boldsymbol{\pi}(2), \cdots, \boldsymbol{\pi}(t-1)$ に加え，時刻 $t-1$ における一人分 $u \in U$ の滞在 POI を背景知識として持つ攻撃者のクラス $\mathsf{OPK}(K_{\mathsf{OPK}}, f_{\mathsf{OPK}}, g_{\mathsf{OPK}})$ を考える．この背景知識は，例えば，攻撃者が攻撃対象を時刻 $t-1$ まで尾行していたが見失い，時刻 t における滞在 POI を推測する場合などを表している．この攻撃者のクラスにおける背景知識は，$K_{\mathsf{OPK}} = \{\boldsymbol{\pi}(t-1), \boldsymbol{P}_1, X_{t-1}^u = \ell_i\}$ である．

[*1] この確率を混合多項分布として求めることはできない．これは，二つの POI からなり遷移確率行列が単位行列であるような場合を考えることでわかる．混合多項分布を用いるとどのようなヒストグラムに対しても実現確率が 0 となってしまう．

我々は，このクラスの攻撃者が出力ヒストグラムの観測前後において，攻撃対象 u が時刻 t に POI ℓ_j に滞在していると推測する確信度 $f_{\mathsf{OPK}}, g_{\mathsf{OPK}}$ を次のように定める．

$$
\begin{aligned}
&f_{\mathsf{OPK}}(u,t,\ell_j,\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,X^u_{t-1}=\ell_i\})\\
&= p(X^u_t=\ell_j|X^u_{t-1}=\ell_i,\tilde{\boldsymbol{\pi}}(t),\boldsymbol{\pi}(t-1);\boldsymbol{P}_1)\\
&= \frac{p(\tilde{\boldsymbol{\pi}}(t),\boldsymbol{\pi}(t-1)|X^u_t=\ell_j,X^u_{t-1}=\ell_i;\boldsymbol{P}_1)p(X^u_t=\ell_j;\boldsymbol{P}_1)}{p(\tilde{\boldsymbol{\pi}}(t),\boldsymbol{\pi}(t-1);\boldsymbol{P}_1)}\\
&g_{\mathsf{OPK}}(u,t,\ell_j,\boldsymbol{\pi}(t),\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,X^u_{t-1}=\ell_i\})\\
&= p(X^u_t=\ell_j|X^u_{t-1}=\ell_i,\boldsymbol{\pi}(t),\boldsymbol{\pi}(t-1);\boldsymbol{P}_1)\\
&= \frac{p(\boldsymbol{\pi}(t-1),\boldsymbol{\pi}(t)|X^u_t=\ell_j,X^u_{t-1}=\ell_i;\boldsymbol{P}_1)p(X^u_t=\ell_j;\boldsymbol{P}_1)}{p(\boldsymbol{\pi}(t-1),\boldsymbol{\pi}(t);\boldsymbol{P}_1)}
\end{aligned}
$$

この時，u が時刻 t に ℓ_j に滞在していると推測する場合の出力 $\boldsymbol{\pi}(t)$ による確信度の贈与は，次の通りである．

$$
\begin{aligned}
&\mathrm{Gain}_{\mathsf{OPK}}(\boldsymbol{\pi}(t),u,t,\ell_j,\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,X^u_{t-1}=\ell_i\})\\
&= \frac{p(\boldsymbol{\pi}(t)-\boldsymbol{e}_j,\boldsymbol{\pi}(t-1)-\boldsymbol{e}_i;\boldsymbol{P}_1)p(\tilde{\boldsymbol{\pi}}(t),\boldsymbol{\pi}(t-1);\boldsymbol{P}_1)}{p(\tilde{\boldsymbol{\pi}}(t)-\boldsymbol{e}_j,\boldsymbol{\pi}(t-1)-\boldsymbol{e}_i;\boldsymbol{P}_1)p(\boldsymbol{\pi}(t),\boldsymbol{\pi}(t-1);\boldsymbol{P}_1)}
\end{aligned}
$$

3.2.3 時刻 t における全員分の滞在 POI を知る攻撃者

OPK クラスを拡張し，時刻 $t-1$ における N 人全員分の滞在 POI を知っている攻撃者のクラス NPK を考える．N 人分の時刻 $t-1$ における滞在 POI を $\boldsymbol{\kappa}(t-1)$ と書くと，このクラスの攻撃者における背景知識は $K_{\mathsf{NPK}}=\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,\boldsymbol{\kappa}(t-1)\}$ となる．このクラスの攻撃者が時刻 t に N 人のうちの一人 $u\in U$ が ℓ_j に滞在していると推測する場合の出力ヒストグラム $\boldsymbol{\pi}(t)$ による確信度の贈与は，$\mathrm{Gain}_{\mathsf{OPK}}(\boldsymbol{\pi}(t),u,t,\ell_j,\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,X^u_{t-1}=\ell_i\})$ である．従って，$\mathsf{NPK}(K_{\mathsf{NPK}},f_{\mathsf{OPK}},g_{\mathsf{OPK}})$ と定義する．このクラスの攻撃者に対して出力がアドバーザリアルプライベートであるためには，N 人中のどの一人に対しても出力がアドバーザリアルプライベートである必要がある．そのためには，贈与の最大値を制限すれば十分である．

よって，公開ヒストグラム $\boldsymbol{\pi}(t)$ が NPK クラスの攻撃者に与える贈与は，次の通りである．

$$
\begin{aligned}
&\mathrm{Gain}_{\mathsf{NPK}}(\boldsymbol{\pi}(t),\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,\boldsymbol{\kappa}(t-1)\})\\
&= \max_{u,\ell_j,\ell_i}\mathrm{Gain}_{\mathsf{OPK}}(\boldsymbol{\pi}(t),u,t,\ell_j,\{\boldsymbol{\pi}(t-1),\boldsymbol{P}_1,X^u_{t-1}=\ell_j\})
\end{aligned}
$$

4. プライバシ保護

本節では，3.2 節で導入した各アドバーザリークラスに対して，アドバーザリアルプライベートであるヒストグラム $\boldsymbol{\pi}^*(t)$ の計算アルゴリズムについて説明する．先ず初めに，二つのヒストグラムの実現確率 (2) の最大値の効率的な計算方法について説明する．その後，アドバーザリアルプライベートかつ元のヒストグラムとの誤差の少ないヒストグラム $\boldsymbol{\pi}^*(t)$ を求めるアルゴリズムを導入する．

4.1 最大実現確率の計算

我々は，二つのヒストグラム $\boldsymbol{\pi}(t-1),\boldsymbol{\pi}(t)$ に矛盾しない N 人分の行動のすべて $\mathcal{A}(\boldsymbol{\pi}(t-1),\boldsymbol{\pi}(t))$ をフローネットワーク G を用いて表現する．このフローネットワークは，ソースノード s，シンクノード e，そして時刻 $t-1$ 及び t における POI 集合 V_{t-1},V_t をノードとする．そして，このノードに対して次のように枝を張る．ソースノード s から $\forall\ell\in V_{t-1}$ に枝を張り，$\forall\ell\in V_t$ からシンクノード e に枝を張る．そして，$P_{i,j}$ が 0 でないとき $\ell_i\in V_{t-1}$ から $\ell_j\in V_t$ に枝を張り，枝集合を E とする．

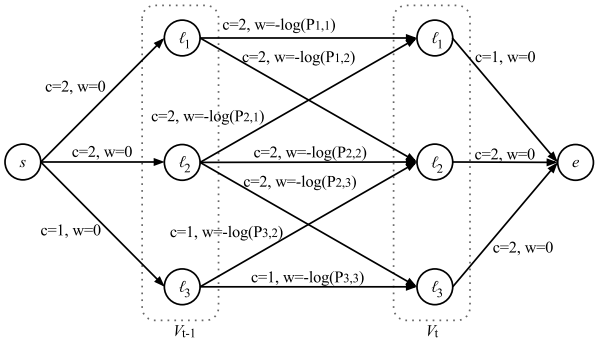


図 1 二つのヒストグラムを表すフローネットワーク
Fig. 1 Flow network of two histograms

例 4.1. マルコフ過程 M_1 が与えられており，$\boldsymbol{\pi}(t-1)=(2,2,1)^t,\boldsymbol{\pi}(t)=(1,2,2)^t$ であるとする．この状況は **図 1** に示すフローネットワークとして表現できる．なお，枝ラベルは後で説明する容量 c 及びコスト w を表している．

このネットワークの各枝に容量を設定する．頂点 u から v に張られた枝を (u,v) と書くと，容量関数 $c:E\to\mathbb{R}^{+*2}$ は，

$$
c(u,v)=\begin{cases}\pi_j(t-1) & ;\text{if } u=s,\ v\in V_{t-1},\\ \pi_i(t-1) & ;\text{if } u\in V_{t-1},\ v\in V_t,\\ \pi_i(t) & ;\text{if } u\in V_t,\ v=e.\end{cases}\qquad(4)
$$

となる．このように容量を定めることで (s,e)-フローネットワーク $G=(s,e,V_{t-1}\cup V_t,E,c)$ において最大流問題を解いて得られるフローは，任意二つの頂点 $\ell_i\in V_{t-1}$，$\ell_j\in V_t$ を結ぶ枝におけるフローが時刻 $t-1$ から t の間に ℓ_i から ℓ_j に移動した人数を表すことになる．

最大流を与えるフローは一般に複数ありうるが，我々は実現確率が最大となる行動 A を得ることが目的のため，各枝にコストを設定し最小コスト最大流問題へ拡張する．最小コスト最大フロー問題では，各枝 (u,v) に設定されたコスト $w(u,v)$ を基に，最大流のうち $w(u,v)f(u,v)$ を最小とするフローを求める問題である．

コスト関数 $w:E\to\mathbb{R}^+$ として

$$
w(u,v)=\begin{cases}0 & ;\text{if } u=s,\ v\in V_{t-1},\\ -\log(P_{i,j}) & ;\text{if } u=\ell_i\in V_{t-1},\ v=\ell_j\in V_t,\\ 0 & ;\text{if } u\in V_t,\ v=e.\end{cases}\qquad(5)
$$

*2 $\mathbb{R}^+$ で非負の実数集合を表す．

Algorithm 1 private histogram

Require: The previouse relased histogram $\boldsymbol{\pi}^*(t-1)$.
Require: Markov transition matrix $\boldsymbol{P}_1$.
Require: Step parameter $s \in (0,1)$.
  $\boldsymbol{\pi}^*(t) \leftarrow \boldsymbol{\pi}(t)$
  $\alpha \leftarrow 0$
  while $\max_{u,\ell_j} \mathrm{Gain}_{\mathsf{NPK}}(\boldsymbol{\pi}^*(t), u, t, \ell_j, K) > e^{\epsilon}$ **do**
    $\alpha \leftarrow \max(\alpha + s, 1)$
    $\boldsymbol{\pi} \leftarrow (1-\alpha)\boldsymbol{\pi}(t) + \alpha\tilde{\boldsymbol{\pi}}(t)$
    $\boldsymbol{\pi}^*(t) \leftarrow N\boldsymbol{\pi}/\|\boldsymbol{\pi}\|$
  end while
  return $\boldsymbol{\pi}^*(t)$

を用いると次の定理が成り立つ．

定理 4.1. (s,e)-フローネットワーク $G_f = (s, e, V_{t-1} \cup V_t, E, c, w)$ の最小コスト最大フローにおけるコストの総和を $C_{\min}$ とすると，$\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t)$ の実現確率の最大値，式 *(3)* は，$p_{\max}(\boldsymbol{\pi}(t-1), \boldsymbol{\pi}(t); \boldsymbol{P}_1) = N! \times \exp(-C_{\min})$．

4.2 アドバーザリアルプライベートなヒストグラムの計算

NPK クラスの攻撃者に対して ϵ-アドバーザリアルプライベートであるヒストグラム $\boldsymbol{\pi}^*(t)$ の導出には，アルゴリズム 1 を用いる．このアルゴリズムは，プライバシ保護を行っていない元々のヒストグラム $\boldsymbol{\pi}(t)$ と，一つ前の時刻の出力 $\boldsymbol{\pi}^*(t-1)$，マルコフ遷移確率行列 $\boldsymbol{P}_1$，そしてステップパラメータ s を入力とする．ヒストグラム $\boldsymbol{\pi}(t)$ が ϵ-アドバーザリアルプライベートでない場合，$\boldsymbol{\pi}(t)$ とマルコフモデルから推測されるヒストグラム $\tilde{\boldsymbol{\pi}}(t) = (\boldsymbol{\pi}(t)^t \boldsymbol{P}_1)^t$ との内分点を出力候補のヒストグラムとする．出力候補が ϵ-アドバーザリアルプライベートでなければ内分点を $\boldsymbol{\pi}(t)$ から $\tilde{\boldsymbol{\pi}}(t)$ に近づけていき，$\max_{u,\ell_j} \mathrm{Gain}_{\mathsf{NPK}}(\boldsymbol{\pi}^*(t), u, t, \ell_j, K) \leq e^{\epsilon}$ を満足した点を出力する．他のクラスの攻撃者に対しては，ループの条件を各クラスで定義された贈与とすることで同様に ϵ-アドバーザリアルプライベートであるヒストグラム $\boldsymbol{\pi}^*(t)$ を求めることができる．

マルコフモデルから推測されるヒストグラム $\tilde{\boldsymbol{\pi}}(t)$ は ϵ-アドバーザリアルプライベートであるため，内分点が $\tilde{\boldsymbol{\pi}}(t)$ に一致すれば要件は満足される．言い換えれば，アルゴリズム 1 は必ず停止する．この手法は，最適なヒストグラムを選択することはできないが，短い時間で近似解を求めることができる．ステップパラメータ s を小さくとることで，より本来のヒストグラム $\boldsymbol{\pi}(t)$ に近い出力を得ることができるが，計算時間のトレードオフがある．

5. 高階マルコフ過程の利用

本節では，2 節で導入した 1 階マルコフ過程 M_1 を拡張した高階マルコフ過程について議論する．1 階マルコフ過程 M_1 では，状態集合 S_1 として POI グラフ G_{POI} の頂点集合 V_{POI} を用いた．この場合，マルコフ過程 M_1 は，ある POI に居た人は次の時刻にどの POI に向かいやすいのかを表している．言い換えれば，POI と POI の関係を表したものであり，移動方向や速度を考慮していない．

例えば，3 つの POI $\{\ell_1, \ell_2, \ell_3\}$ を考える．そして，ℓ_1 から ℓ_2 と移動した人が次に ℓ_3 に向かう確率と ℓ_3 から ℓ_2 と移動した人が次に ℓ_3 へ戻る確率が異なる場合を考える．すなわち，1 次マルコフ仮定が成り立たない場合，当然ながらマルコフ過程 M_1 を利用することはできない．

このような状況を扱うためには，各時刻に滞在している POI だけではなくその前の時刻に滞在していた POI も併せた POI のペアを状態として持つ 2 階マルコフ過程 $M_2(S_2, \boldsymbol{P}_2)$ を用いる．M_2 における状態集合 S_2 は，POI グラフ G_{POI} においてヒストグラムの公開間隔 Δt で移動可能な POI ペア集合 $S_2 \subseteq V_{\mathrm{POI}} \times V_{\mathrm{POI}}$ となる．また，遷移確率 P_2 は Δt によって定まり，与えられるものとする．このマルコフ過程 M_2 に対しても 4 節までの議論はそのまま成り立ち，各時刻に POI ペアすなわち 2 グラムの遷移を行った人数のカウントを ϵ アドバーザリアルプライベートなヒストグラム $\boldsymbol{\pi}(t)$ として公開することができる．

同様にして，n 階マルコフ過程 $M_n(S_n, \boldsymbol{P}_n)$ を考えることができる．M_n では，状態集合 S_n は $S_n \subset V_{\mathrm{POI}}^n$ となり[*3]，遷移確率 P_n は Δt によって定まり，$\boldsymbol{P}_1, \boldsymbol{P}_2$ 同様に与えられるものとする．このマルコフ過程 M_n に対しても今までの議論は成り立つ．マルコフ過程 M_n を採用した場合，出力は各時刻における長さ n のパスのカウントになる．従って，各 POI における滞在人数だけではなく，パス情報が求められる場合でも我々の提案手法は有効である．

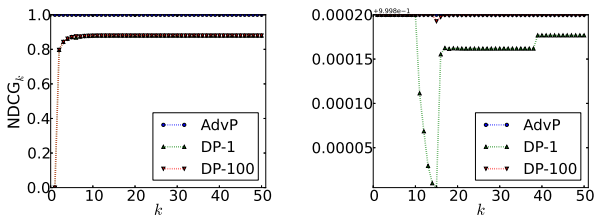
6. 評価実験

出力データを用いた解析として頻出パス検出を想定し，高階マルコフ過程を用いた場合の出力を評価した．データセットは，人の流れプロジェクト[*4]にて公開されている東京都市圏（1998 年）データのうち，都市部データセットとして渋谷駅周辺 14 駅，郊外データセットとして町田駅周辺 14 駅を POI とし鉄道移動を行った人々の行動記録からなるたデータセットである．渋谷駅周辺では 2062 人分，町田駅周辺では 683 人分の 24 時間のデータからなる．

比較手法として，差分プライバシを満たすパスを出力する Chen らの手法 [3] を用いた．[3] によれば，一般的に解析に用いられるパスの長さは 5 程度であるとのことであり，本実験でもパスの長さは 5 とした．そのため，提案手法でも 5 階マルコフ過程 M_5 を用いて長さ 5 のパスに対するカウントをヒストグラム $\boldsymbol{\pi}(t)$ として出力した．比較手法は 24 時間分の集約結果を入出力とするが，我々の提案手法では，1 分間隔でヒストグラムを出力した．そして，得られた 1440 分の和を集約結果として用いた．

得られたパスとそのカウントを用いた解析タスクとし

*3 $V^1 = V$ として $V^n = V \times V^{n-1} (n \geq 2)$ と定義する．
*4 http://pflow.csis.u-tokyo.ac.jp/



(a) 渋谷駅周辺　　(b) 町田駅周辺

図 2 NDCG の比較
Fig. 2 Comparision of NDCG

て，[3] 同様に頻出パス発見を想定し，頻出パスランキングを作成することとした．頻出パスランキングの質を評価するために，NDCG [8] を用いた．トップ k ランキングの NDCG，NDCG_k は，$\mathrm{NDCG}_k = \mathrm{DCG}_k/\mathrm{IDCG}_k$ と定義される．ここでは，DCG として $\mathrm{DCG}_k = \sum_{i=1}^{k} \frac{2^{rel_i}-1}{\log(1+i)}$ を用いた．なお，rel_i はパス i の正解ランキング，すなわち匿名化処理を行う前のデータから得られた頻出パスランキングにおけるランクを $rank_i^*$ として，$rel_i = k - rank_i^*$ とした．IDCG は，正解ランキングの DCG である．NDCG は 0 から 1 までの値を取り，大きい値ほどトップ k ランキングが正解ランキングに近いことを表す指標である．

図 2 は，提案手法 (AdvP)，$\epsilon = 1,100$ とした差分プライバシ（DP-1, DP-100）を満足する出力情報から頻出パスランキングを計算しその NDCG を比較したものである．図の横軸はトップ k 件の k を，縦軸は NDCG_k を表す．

提案手法用いたデータから作成した頻出パスランキングは，正解ランキングとほぼ変わらない結果となっていることが分かる．これは，1 節で述べたように，移動履歴から作成するパス情報がスパース性を持ち，我々の提案手法が稀だがマルコフ過程的に自明な遷移を行う POI (ここでは稀なパス) については，プライバシ保護を行わないことによる．すなわち，情報には稀なパスが多く含まれるというスパース性があるが，それらについてはプライバシ保護は行わず，頻出なパスのみにプライバシ保護を行っているため全体としてノイズの少ない結果を得ることができている．

一方，差分プライバシを満足するデータから作成した頻出パスランキングは，ϵ にあまり依存せず，渋谷駅周辺ではトップ数件以外は正しいランキングとなっており，町田駅周辺では，多少の誤差はあるもののほぼ正しいランキングとなっている．これは，SDS が頻出ではないパスを予め削除してから差分プライバシを適用するアルゴリズムであり，パスカウントのスパース性の影響を受けにくいアルゴリズムであるからである．しかし，逆位に言えば稀なパスは出力できないため解析用途が限定される．我々の手法は，稀なパスであっても出力するため用途を選ばない．

7. まとめと今後の課題

本論文では，プライバシを保護しつつ位置情報を継続的に公開するためのマルコフ性を仮定したアドバーザリアルプライバシを提案した．評価実験では，公開位置情報を用いた解析タスクとして頻出パス抽出を想定し，提案手法による出力ヒストグラムと差分プライバシを満たす出力ヒストグラムによる解析結果を比較した．我々が提案するアドバーザリアルプライバシは，差分プライバシのようにどのような背景知識を仮定しない攻撃者に対してもプライベート性を保証するわけではないが，3.2 節で定義した各攻撃者のクラス対してプライベートな出力を与える．その上でより正確な解析結果を得ることができた．今後の課題は，提案手法の大規模データへの利用であり，スケーラブルな最小コスト最大フロー問題の解法を考えている．

謝辞 本研究は最先端研究開発プログラム (FIRST)「超巨大データベース時代に向けた最高速データベースエンジンの開発と当該エンジンを核とする戦略的社会サービスの実証・評価」の助成を受けたものである．

参考文献

[1] Dwork, C., Mcsherry, F., Nissim, K. and Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis, *Proc. of the Third Theory of Cryptography Conference*, Springer, pp. 265–284 (2006).
[2] Chen, R., Mohammed, N., Fung, B. C. M., Desai, B. C. and Xiong, L.: Publishing Set-Valued Data via Differential Privacy, *Proc. of the 37th International Conference on Very Large Data Bases*, Vol. 4, No. 11, VLDB Endowment, pp. 1087–1098 (2011).
[3] Chen, R., Acs, G. and Castelluccia, C.: Differentially Private Sequential Data Publication via Variable-Length N-Grams, *Proc. of the 19th ACM Conference on Computer and Communications Security*, ACM Press, pp. 638–649 (2012).
[4] Rastogi, V., Hay, M., Miklau, G. and Suciu, D.: Relationship Privacy: Output Perturbation for Queries with Joins, *Proc. of the 28th ACM Symposium on Principles of Database Systems*, ACM Press, pp. 107–116 (2009).
[5] Mannini, A. and Sabatini, A. M.: Accelerometry-based classification of human activities using Markov modeling., *Computational Intelligence and Neuroscience*, Vol. 2011 (2011).
[6] Kifer, D. and Machanavajjhala, A.: No Free Lunch in Data Privacy, *Proc. of the 2011 ACM SIGMOD International Conference on Management of Data*, ACM Press, pp. 193–204 (2011).
[7] Götz, M., Nath, S. and Gehrke, J.: MaskIt: Privately Releasing User Context Streams for Personalized Mobile Applications, *Proc. of the ACM SIGMOD International Conference on Management of Data*, ACM Press, pp. 289–300 (2012).
[8] Järvelin, K. and Kekäläinen, J.: IR evaluation methods for retrieving highly relevant documents, *Proc. of the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, ACM Press, pp. 41–48 (2000).