Vol.2015-DPS-163 No.12
Vol.2015-MBL-75 No.12
2015/5/28

時変動する動的な人口密度分布を考慮した位置プライバシ保護に関する性能評価と課題の検討

松野 有弥[1]　青木 俊介[1]　伊藤 昌毅[2]　瀬崎 薫[2,3]

概要：GPS 機能が搭載された携帯端末の普及に伴い，ユーザの位置に対応する情報を提供する位置情報サービスが多数展開されている．しかし，位置情報サービスを利用する際には，ユーザは自身の位置情報をサービスプロバイダへ送信する必要があり，位置情報が第三者に取得されることで，プライバシが侵害される可能性が大きな課題となっている．時空間統計情報から個人の移動特性や行動パターンなどを推測する研究が多数展開されており，その有効性が示されている．そこで本研究では，時変動する動的な人口密度分布を位置プライバシの問題に適用することの有効性を評価し，位置プライバシ保護の問題に対する影響や課題について検討する．

キーワード：位置プライバシ，位置情報サービス，人口密度分布

Study on Location Privacy Preservation Considering Time Variation of Population Density

Abstract: The diffusion of mobile devices equipped with global positioning system(GPS) has made available various services providing useful information related to the user's location. Since the users have to send their location information, preserving location privacy has become a significant challenge. There are a lot of studies to estimate the movement properties and behavior pattern which could be location privacy threat. In this paper, we evaluate the effectiveness of considering time variation of population density for the issue of location privacy preservation.

Keywords: Location Privacy, Location Based Service, Population Density

1. はじめに

近年の GPS をはじめとする位置測位技術の発展に伴い，ユーザの位置に対応する情報やサービスを提供する位置情報サービスが数多く展開されている．位置情報サービスプロバイダは，位置検索，経路探索，近隣店舗のクーポンなどの広告情報などのユーザの位置に関する様々なサービスを提供している．サービスプロバイダが提供する利便性を享受するためには，ユーザは自身の位置情報をサービスプロバイダに送信しなければならず，位置情報が第三者に取得されることにより，ユーザの行動パターンや健康状態などの位置情報に紐付く個人情報が把握されるなど，プライバシが侵害される問題が課題となっている．

このような位置情報に関するプライバシの保護を目的とした研究は数多く行われている．M. Gruteser らは，ユーザが自身の位置情報を直接サービスプロバイダに送らずに，自身と他の $k-1$ 人のユーザを含むような領域に対するクエリをサービスプロバイダに送信する k-匿名化処理を施す手法を提案している [1]．これにより，攻撃者は k 人の位置情報から $\frac{1}{k}$ 以上の確率でユーザの位置を識別することができない．また，L. Huang らは，silent period という設定された期間内に他のノードと ID を交換または変更する手法を提案している [2]．これにより，ID 更新前後の時空間情報の関連性を低下させることが可能となる．さら

[1] 東京大学 大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
[2] 東京大学 生産技術研究所
Institute of Industrial Science, The University of Tokyo
[3] 東京大学 空間情報科学研究センター
Center for Spatial Information Science, The University of Tokyo

に，自身の位置情報とともに偽の位置情報を付加してサービスを要求するダミーの位置情報を用いた手法 [3] や，代替地点の位置情報を付加したり，位置情報の精度を低下させてユーザの位置の曖昧性を高める手法の研究などが盛んに行われている [4]．位置情報サービス利用環境や条件を規定した上で，位置プライバシ保護のための評価指標を基に様々な位置プライバシ保護手法が提案されており，位置プライバシ保護を的確に評価することができる指標の検討も重要である [5]．

また，無線通信技術の進歩によって，時空間情報から統計情報を取得する技術も近年注目を集めている．時空間統計情報から人口動態を把握したり，自宅や勤務先などの位置情報をはじめとする個人情報を推測する研究が盛んに行われており，その有効性が示されている [6–9]．このような時空間的に細粒度の人口密度分布などの人口動態や個人の移動特性などの推定技術は，既存の位置プライバシ保護手法の機能低下につながる可能性があり，脅威と成り得る．

そこで，本研究では，ユーザがある位置で位置情報サービスを利用し，次のサービス利用位置まで移動するような，散発的に位置情報サービスを利用する移動モデルを想定して，文献 [10,11] で述べられている位置プライバシ保護評価フレームワーク [12] を用いて，時変動する動的な人口密度分布が位置プライバシ保護の問題に与える影響を調査する．この位置プライバシ保護評価フレームワークでは，ユーザの位置を推測しようとする攻撃者は，予めユーザの位置情報履歴を取得したり，通信を不正に傍受することでユーザの移動についての事前情報を蓄積することが可能であるとする．また，位置を状態とするマルコフ連鎖でユーザの移動をモデル化できると想定しており，事前情報からユーザの位置に関する遷移確率を算出し，新たに観測されるプライバシ保護処理済みの移動軌跡を利用して，ユーザの実際に位置する領域についての確率分布を推定する．この推定確率分布を攻撃者のユーザ位置の推定能力とみなし，これを利用することで位置プライバシ保護レベルを定量化し評価する．この攻撃者の推定確率分布に対して，時変動する動的な人口密度分布から得られる，各領域に人が存在する事前確率分布を掛け合わせることで，攻撃者の推定能力にどのような影響を与えるかを調査する．そして，位置プライバシ保護の問題に与える影響や課題について検討する．

以下では，2 章で関連研究を説明し，3 章で本研究で使用する位置プライバシ保護評価フレームワークについて述べる．4 章で時変動する動的な人口密度分布を考慮した位置プライバシ保護に関する性能評価の結果を示し，最後に 5 章で本稿のまとめと今後の課題について述べる．

2. 関連研究

本章では，時空間情報から人口動態統計を取得したり，個人の移動軌跡や行動パターンなどを推定することを目的とした研究について述べる．

文献 [6] では，匿名化された GPS 移動データから個人を識別して，自宅の位置を推定する手法を提案している．約 60m の誤差で推定可能であるとしており，3 つの異なるプライバシ保護手法に対して，この位置推定手法への有効性を評価している．また，文献 [7] では，個人の移動履歴から停止位置の意味的情報に関して頻出するパターンを抽出する手法が提案されている．時空間情報だけではなく停止位置の意味的な情報を考慮することで，停止位置の予測精度を向上している．さらに，文献 [8] では，匿名化された携帯電話の呼詳細情報 (CDR : Call Detail Record) を解析することで，個人の自宅や勤務先などの重要な位置情報や行動パターンを識別する手法が提案されている．また，文献 [9] では，CDR からは観測できない学生や子どもなどの携帯端末を持たない人口を把握するため，子どもと移動を共にする男女の通信位置の傾向を分析している．

個人の移動履歴から抽出される特徴と時空間情報を利用した位置推定手法を考慮して，位置プライバシ保護手法を構築する研究は多数展開されている．しかし，個人の移動は人々の流動状況からも影響を受けることがあり，その時々により日常とは異なる移動を行う可能性がある．そして，個人の移動履歴から位置推定をすることで個人の位置を特定しようとする攻撃に対するプライバシ保護に関する研究は多数展開されているが，大規模な時空間統計情報を利用して位置を特定する攻撃に対するプライバシ保護に関する研究は行われていない．よって，本研究では，時変動する動的な人口密度分布が既存の位置プライバシ保護手法に与える影響を検証することを目的とする．

3. 位置プライバシ保護評価フレームワーク

本章では，文献 [10,11] で示されている確率的に位置プライバシ保護手法を評価するためのフレームワーク [12] の概要を説明し，本研究における想定環境について述べる．まず，ユーザについての想定と位置プライバシ保護の仕組みについて説明した後，攻撃者の時空間情報推定方法と位置プライバシ保護のための評価指標について述べる．また，図 1 に，この位置プライバシ保護評価フレームワークを示す．

3.1 ユーザ

M 個に分割された領域 $R = \{r_1, r_2, ..., r_M\}$ 内を移動する N 人のユーザ $U = \{u_1, u_2, ..., u_N\}$ を想定する．ユーザは時刻 $T = \{1, .., T\}$ ごとにサービスプロバイダと通信し，自身が現在位置する領域 $r \in R$ を通知することで，その時刻における自身が位置する領域に関する情報やサービスを享受する．ここでは，ユーザ u の時刻 t における実際の時空間情報を $a_u(t) =< u, t, r >$ とし，すべての時刻について実際の時空間情報を時系列順に並べたもの

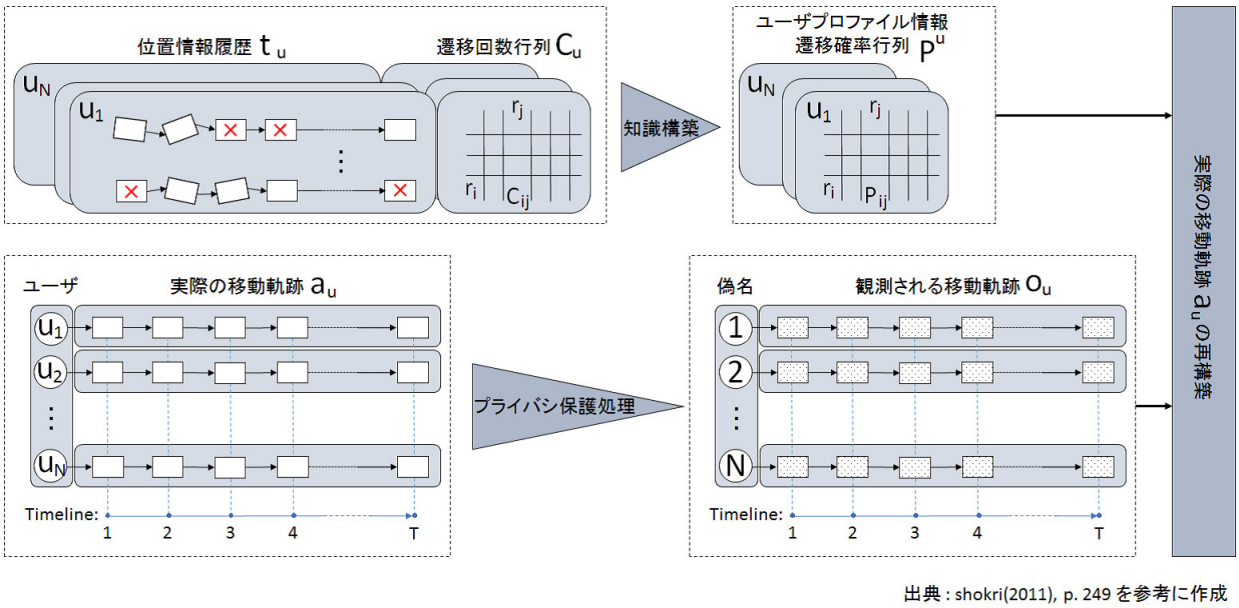


図 1 位置プライバシ保護評価フレームワーク

$a_u = (a_u(1), a_u(2), ..., a_u(T))$ をユーザ u の実際の移動軌跡とする．

3.2 位置プライバシ保護の仕組み

位置プライバシ保護処理を担う機関が N 人の実際の移動軌跡 $\{a_{u_1}, a_{u_2}, ..., a_{u_N}\}$ を受け取り，それぞれの実際の移動軌跡に対して，以下に示すように二段階に分けて位置プライバシ保護手法を適用する．

(1) ユーザ位置の曖昧化
(2) ユーザ ID の交換

まず，手順 (1) で移動軌跡の各時刻におけるユーザの位置情報を実際とは異なる位置情報へと変換することでユーザ位置を曖昧化し，手順 (2) で N 人分の移動軌跡に付与されているユーザ ID を交換することで偽名化を実現する．手順 (1) では，各時刻におけるユーザが実際に位置する領域 $r \in R$ を式 (1) に示すような確率分布に従って偽の領域 $r' \in R$ に変換する．

$$f(r'|r) = Pr\{o(t) =< t, r' > |a(t) =< t, r >\} \qquad (1)$$

ここでは，すべてのユーザの時空間情報に対して同様の確率分布を用いているためユーザについての表記を省略している．また，位置曖昧化処理は設定される割合に基づき各時刻の位置情報に対して，以下に示す 2 種類の方法のうちどちらか一方が適用される．

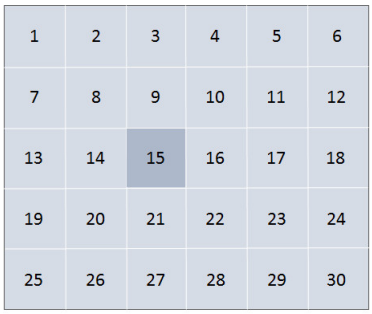
(i) 位置情報を隠蔽する．
(ii) 複数の位置情報を付与する．

処理 (i) では，ユーザの位置情報を付与せずに隠蔽することで $r' = \emptyset$ に変換する．また，処理 (ii) では，実際にユーザが位置する領域 r を含む複数の領域を併合することで $r' = \{r\}$ に変換する．ここでは，自然数で表される位置曖昧化レベルを設定し，その平方数分だけ領域を割り当てる．図 2 に具体例を示す．これらの処理により，サービスプロバイダは時空間情報 $o_u(t) =< u, t, r' >$ を観測することになる．(i) の処理を施す確率を位置隠蔽確率として位置プライバシ保護処理の水準を調整する．

次に，手順 (2) で，位置曖昧化処理後の移動軌跡に対して，N 人分のユーザ ID から無作為に選び出した偽の ID を付与する．以上より，プライバシ保護処理済みであり，ユーザ u の位置推定のために観測される移動軌跡は $o_u = (o_u(1), o_u(2), ..., o_u(T))$ と表わされる．

3.3 攻撃者

次に，ユーザと通信をやりとりするサービスプロバイダ，または，ユーザとサービスプロバイダ間の無線通信を傍受する第三者機関をユーザの時空間情報を不正に取得しようとする攻撃者と想定する．攻撃者は予めユーザの位置情報履歴を取得したり，不正に通信を傍受することでユーザの移動についての事前情報を蓄積することが可能であるとする．また，攻撃者はユーザの移動を領域 R を状態としたマルコフ連鎖でモデル化できると想定しており，文献 [10,11] で説明されているアルゴリズムを利用して，ユーザの位置情報履歴 $t_u = (t_u(1), t_u(2), ..., t_u(T))$ と領域から領域への遷移回数行列 C_u からユーザプロファイル情報 P^u を獲得する．このユーザプロファイル情報 P^u は，ij 成分を領域 r_i から次の時刻で領域 r_j に遷移する確率とする遷移確率行列で示される．ここでは，1 日のうち，時間帯によって異なる移動パターンを人間は有していることを考慮して，サービス利用時刻を昼間や夜間などの時間帯ごとに分類することで，各々の時間帯について領域間の遷移確率を算出している．すなわち，ユーザプロファイル情報 P^u は領域



出典 : shokri(2011), p. 250 を参考に作成

図 2 位置曖昧化処理の具体例
実際にユーザが位置する領域が $r = 15$ であると想定すると，変換後の領域 r' は，処理 (i) では $r' = \emptyset$ に，処理 (ii) では，位置曖昧化レベルを 2 とした場合，$r' = \{15, 16, 21, 22\}$ に変換される．また，ダミーの位置情報を付加する場合は $r' = \{11, 15, 28\}$ に，代替地点に変換する場合は $r' = 9$ に変換される．

についてだけでなく，時間帯についても特徴付けられた状態をもつことになり，時間依存性のある情報とみなすことができる．この時間依存性はユーザの位置プライバシについての要求に対しても影響を与えると考えられる．以下では，簡単のため，すべての場合において，ある 1 つの時間帯について述べているものとする．

攻撃者は，取得したユーザの移動に関する遷移確率で表されるユーザプロファイル情報 P^u と，新たに観測されるプライバシ保護処理済みの移動軌跡 o_u から，実際の移動軌跡 a_u の再構築を試みる．また，攻撃者はユーザが適用する位置プライバシ保護処理に用いられる，式 (1) で示した領域を変換するための確率分布を把握しているものと想定する．ユーザプロファイル情報 P^u が得られ，ユーザ u のプライバシ保護処理済みの移動軌跡 o_u が観測されるという条件の下で，文献 [10, 11] で説明されているアルゴリズムを利用して，式 (2) で示すような，時刻 t においてユーザ u が実際に位置する領域 $a_u(t) = r$ $(r \in R)$ についての事後確率分布を算出することにより，ユーザが実際に位置する領域を推定する．

$$Pr\{a_u(t) = r | o_u, P^u\} \tag{2}$$

3.4 評価指標

評価指標として，式 (3) で定義される，ユーザ u が時刻 t に位置する領域についての攻撃者の推定誤差 $LP(u,t)$ を用いる．ユーザ u の時刻 t における実際に位置する領域を $a_u(t)$，時刻 t においてユーザ u が位置する領域を r と攻撃者が推定する確率を $\hat{p}_{u,t}(r)$ とする．ここで，$\hat{p}_{u,t}(r) = Pr\{a_u(t) = r | o_u, P^u\}$ である．また，$||r - a_u(t)||$ は，ユーザが実際に位置する領域と攻撃者が推定する領域との距離を表しているが，本研究では，$r = a_u(t)$ のように，攻撃者が，正確にユーザが位置する領域を推定するような場合には 0 を，それ以外の，ユーザが位置する領域を誤って推定する場合には 1 をとるものとする．

$$LP(u,t) = \sum_{r \in R} \hat{p}_{u,t}(r) ||r - a_u(t)|| \tag{3}$$

式 (3) から明らかなように，ユーザが実際に位置する領域と攻撃者が推定する領域との距離に関する誤差の期待値を利用することで，位置プライバシの保護レベルを定量化している．したがって，ユーザが実際に位置する領域を攻撃者が正確に推定する確率が高ければ高いほど，$LP(u,t)$ は 0 に近づき，ユーザの位置プライバシ保護レベルは低下する．

本研究では，以上に示したフレームワークを用いて，時変動する動的な人口密度分布を位置プライバシの問題に適用することの有効性を検証する．

4. 時変動する動的な人口密度分布を考慮した位置プライバシ保護に関する性能評価

本章では，プライバシ保護の観点から人々の移動の問題について述べ，時変動する動的な人口密度分布を利用して人々の流動を考慮する攻撃者について説明した後，評価実験について述べる．

4.1 人々の移動の問題

GPS や CDR などの技術革新に伴い，時々刻々と変動する人々の移動を計測することが可能となってきている．生活上必要となる移動を行いながら人々は暮らしており，東京都市圏では，朝の通勤時間帯に郊外から都心部へ多くの人々が流入し，夕方から夜にかけて郊外へと流出していく様子が観測されている [13]．職業，年齢，居住地などの個人の属性から，時間帯別に移動の目的や地域ごとの人々の移動の傾向をある程度推測することが可能である．例えば，自宅がある郊外から勤務先のある都心へ通勤する人々は，朝夕の通勤時には，新宿駅や渋谷駅などが位置するビジネスの中心地であり人口が集中する領域を経由する可能性が高い．このような場合，位置情報サービスを利用する際にユーザ側で自身の位置情報にプライバシ保護処理を施したとしても，変換後の位置が個人の属性とサービス利用時間帯から考えて不自然であるならば，その位置情報はユーザが実際に位置するものではないと容易に推測可能である．

4.2 時変動する動的な人口密度分布を考慮した攻撃者

攻撃者は，3.4 節で述べた通り，ユーザの移動に関する遷移確率であるユーザプロファイル情報 P^u，新たに観測されるプライバシ保護処理済みの移動軌跡 o_u および式 (2) で表わされる各時刻におけるユーザ u が実際に位置する領域 r についての事後確率分布を算出した上で，各時刻における人口密度分布から算出した事前確率分布 $pd_t(r)$ を掛け合わせて正規化した，式 (4) のような確率分布を用いてユーザの位置を推測する．

表 1　パラメータ

パラメータ	範囲
サービス利用間隔 [$hour$]	1
評価対象時間	[0:00, 23:00]
領域 [m^2]	30000^2
総ユーザ数 N[人]	5
位置曖昧化レベル [α]	1, 2, 3, 4
位置隠蔽確率 [β]	0.1, 0.3, 0.5, 0.7
試行回数 [回]	200
評価回数 [回]	1000

$$\frac{\hat{p}_{u,t}(r) \times pd_t(r)}{\sum_{r \in R}(\hat{p}_{u,t}(r) \times pd_t(r))} \tag{4}$$

4.3　評価実験

時変動する動的な人口密度分布から得られる事前確率を考慮することの有効性を確認するために，東京大学空間情報科学研究センターが提供している東京都市圏の人の流れデータセット [13] を用いて，平日の午前 0 時から午後 23 時における実際の人の移動を再現し，評価実験を行った．東京駅を中心とする 30km 四方の領域を 10×10 の格子状に分割し，ユーザが移動する領域とした．人の流れデータセットから 1 時間ごとに位置情報を取得し，100 領域を対象として時変動する動的な人口密度分布を取得した．評価実験に利用する個人の位置情報履歴 t_u と実際の移動軌跡 a_u も同様に人の流れデータセットから取得した．正確には，同一個人の複数の異なる日における移動データの一方を位置情報履歴 t_u，もう一方を実際の移動軌跡 a_u とするべきであるが，今回は両方とも同じデータを用いた．シミュレーションにおける各パラメータは表 1 のように定めた．ここでは簡単のため，位置曖昧化レベルを α，位置隠蔽確率を β で表す．一回の試行で N 人のユーザそれぞれに対して位置プライバシ保護レベルを評価している．位置プライバシ保護処理に用いる位置曖昧化レベル α と位置隠蔽確率 β は表 1 の値を組み合わせて設定した．

4.4　評価指標

本実験では，以下の二つの評価指標を用いて，プライバシ保護処理のレベルを変化させて位置プライバシ保護手法の性能を比較する．

(1) 既存評価指標

ユーザが実際に位置する領域に関する事後確率分布から推定した領域と実際の領域との推定誤差の期待値から位置プライバシを定量化して評価する，式 (3) で示した評価指標．

(2) 提案評価指標

ユーザが実際に位置する領域に関する事後確率分布に，4.2 節で示した時変動する動的な人口密度分布から取得した事前確率分布 $pd_t(r)$ を掛け合わせることにより算出した確率分布を用いて，ユーザが実際に位置する領域についての推定誤差の期待値から位置プライバシを定量化して評価する，式 (5) に示す評価指標．

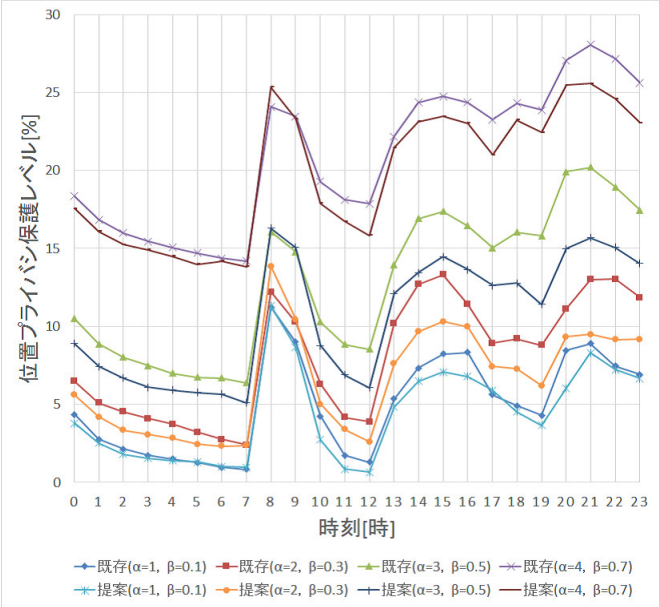


図 3　プライバシ保護レベルの時系列推移

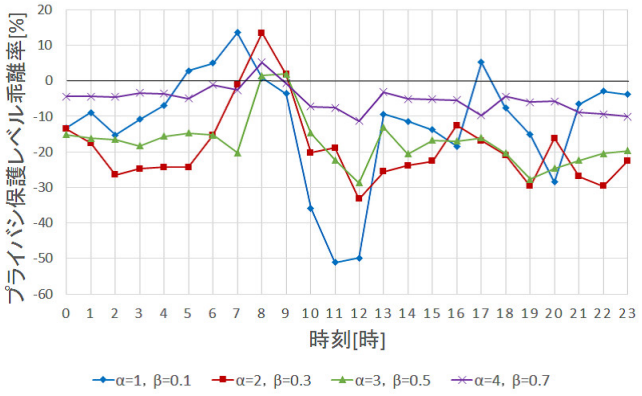


図 4　プライバシ保護レベル乖離率の時系列推移

$$LP_{pd}(u,t) = \sum_{r \in R} \frac{\hat{p}_{u,t}(r) \times pd_t(r)}{\sum_{r \in R}(\hat{p}_{u,t}(r) \times pd_t(r))} ||r - a_u(t)|| \tag{5}$$

4.5　実験結果

様々な水準のプライバシ保護処理を加えた移動軌跡データに対して，4.4 節で述べた二つの評価指標を基にユーザの位置プライバシ保護レベルを定量化した．その結果を図 3，図 4 に示す．ここで，各評価指標から得られる，ユーザが実際に位置する領域についての推定誤差の期待値を百分率で表したものを位置プライバシ保護レベルとして，その時系列推移の様子を図 3 に，また，時変動する動的な人口密度分布を考慮していない既存評価指標に対する，提案評価指標から得られる位置プライバシ保護レベルの乖離率の時系列推移の様子を図 4 に示す．

すべてのプライバシ保護処理水準に関して，深夜から早朝にかけて位置プライバシ保護レベルは低い水準で推移している．そして，通勤時間帯である午前 7 時から 9 時頃にかけて位置プライバシ保護レベルは増加し，その後，正午に近づくにつれて徐々に低下していく．さらに，正午を境に位置プライバシ保護レベルは増加していき，夕方に低下した後，帰宅時間帯に差し掛かるとまた増加していることがわかる．さらに，帰宅後から深夜にかけて位置プライバシ保護レベルは低下している．これは，深夜から早朝にかけて人々は自宅に留まり移動しないことにより，攻撃者が容易に位置を推定することが可能であるからである．通勤時間帯にさまざまな領域間を移動することで，攻撃者の推定確率分布が偏ることなくランダムに分配されるので，攻撃者の推定精度が低下している．勤務地に到着すると，一般的にその場に留まり仕事をすることから，勤務地が含まれる領域を推定する確率が高くなり，攻撃者の推定性能が段々と向上していると考えられる．また，正午を過ぎると移動をする機会が増え，攻撃者の推定確率分布がランダムに分配される傾向が高くなり，攻撃者の推定性能が低下していく．帰宅時間帯に差し掛かると人々は帰路に就くので移動が頻繁に起こり，攻撃者の推定性能が低下していく．しかし，一般的に自宅にいる考えられる時間帯に差し掛かると，早朝と同様に，人々はその場に留まり移動しなくなるので，同一の領域の情報が蓄積され，攻撃者の推定性能が向上するので，位置プライバシ保護レベルは低下していくと考えられる．

図 4 に示した，既存評価指標に対する提案評価指標から得られる位置プライバシ保護レベルの乖離率について，それぞれのプライバシ保護処理水準の結果から，ほとんどの時刻でプライバシ保護レベルが低下していることがわかる．図 3，図 4 からも明らかなように，通勤時間帯である午前 7 時から 8 時頃にかけて，人口密度分布を考慮して評価したプライバシ保護レベルが既存評価指標で評価したプライバシ保護レベルを上回る現象が生じている．これは，一日のうち通勤時間帯は特定の領域に人口が集中するので，非常に偏った事前確率分布を形成しやすいことが原因である可能性が高い．人口密度分布から形成される事前確率分布により，実際にユーザが位置しない領域を指し示す確率が大きくなり推定誤差が拡大していくことも原因として挙げられる．

また，位置プライバシ保護レベルを時系列に捉えず，観測時間全体の平均値として表したものが表 2 である．この表 2 が示す結果から，プライバシ保護処理水準が (α=1, β=0.1) の場合，提案評価指標では，既存の評価指標と比べ約 11%ほど位置プライバシ保護レベルが低下している．さらに，プライバシ保護処理水準を上げていくと，(α=2, β=0.3) の場合では 18%，(α=3, β=0.5) の場合では 17%ほど，位置プライバシ保護レベルが大きく低下している．しかし，プライバシ保護処理水準が一番高い (α=4, β=0.7) の場合，位置プライバシ保護レベルの低下は 5%ほどと小さい．これは，攻撃者の推定性能が低下するに従い，実際にユーザが位置する領域付近に重みづけされた推定確率分布が得られない可能性も高くなり，人口密度分布から得られる事前確率分布の各領域における重みを反映すると，全く異なる領域に確率が分布する可能性があることも原因の一つであると考えられる．

表 2 位置プライバシ保護レベルと乖離率の平均値

	位置プライバシ保護レベル
既存 (α=1, β=0.1)	0.04950
提案 (α=1, β=0.1)	0.04418
既存 (α=2, β=0.3)	0.08033
提案 (α=2, β=0.3)	0.06548
既存 (α=3, β=0.5)	0.1284
提案 (α=3, β=0.5)	0.1062
既存 (α=4, β=0.7)	0.2094
提案 (α=4, β=0.7)	0.1982
	乖離率 [%]
(α=1, β=0.1)	-10.7429
(α=2, β=0.3)	-18.4867
(α=3, β=0.5)	-17.3122
(α=4, β=0.7)	-5.3512

4.6 位置プライバシ保護への課題の検討

本節では，評価実験から得られた結果をもとに位置プライバシ保護に関して，時変動する動的な人口密度分布が与える影響について述べる．図 3，図 4 に示した通り，さまざまな水準のプライバシ保護手法に対して，時変動する動的な人口密度分布を考慮することにより，位置プライバシ保護手法の機能低下を確認した．これは，人口が密集している領域についての重みを攻撃者の推定確率分布に反映することにより，位置曖昧化処理により広域に拡大された位置情報をサービスプロバイダへ送信して自身の位置を曖昧化しても，統計的に人々が集まる領域を移動する傾向があるならば，攻撃者は推定性能を向上させることができる．しかし，人々は生活上必要となる移動を日々繰り返して日常生活を送っており，攻撃者の推定性能を向上させる人口密度分布を自身で構成しながらも，日々の行動パターンを変えるのには大きな苦痛が伴う．逆に，人々が統計的に密集しやすい領域を経由せずに日々移動しているならば，攻撃者の推定性能への影響は乏しい可能性がある．すなわち，統計的に人々が密集する地域や，駅や交通機関などを頻繁に経由せざるを得ない人々にとって，時変動する動的な人口密度分布が攻撃者の位置推定能力に与える影響は脅威となる可能性がある．

5. おわりに

本項では，位置情報サービス利用におけるユーザの位置プライバシ保護の問題に，時変動する動的な人口密度分布

を適用することの有効性を検証した．確率的に位置プライバシ保護手法を評価する既存のフレームワークを用いて，時変動する動的な人口密度分布を，領域ごとの事前確率分布として利用する位置プライバシ評価指標を提案し，位置プライバシ保護処理済みの移動軌跡データを用いてシミュレーション実験を行った．

評価実験の結果，すべてのプライバシ保護処理水準において，時変動する動的な人口密度分布を考慮することで位置プライバシ保護レベルが低下し，既存の位置プライバシ保護手法の機能が低下していることを確認した．

今回は，ユーザが実際に位置する領域についての攻撃者の推定誤差の期待値から位置プライバシ保護レベルを評価したが，今後は，他の位置プライバシ保護手法への時変動する動的な人口密度分布の影響を調査する予定である．さらに，今回得られた課題をもとに，人々の日常における移動をはじめとして，個々人の属性に特有の移動や，災害や台風などの突発的な事象による人々の移動を捉え，位置プライバシの問題として定量的に評価することができる枠組みの構築を検討している．

参考文献

[1] Gruteser, M. and Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking, *Proceedings of the 1st international conference on Mobile systems, applications and services*, ACM, pp. 31–42 (2003).

[2] Huang, L., Matsuura, K., Yamane, H. and Sezaki, K.: Enhancing wireless location privacy using silent period, *Wireless Communications and Networking Conference, 2005 IEEE*, Vol. 2, IEEE, pp. 1187–1192 (2005).

[3] Kido, H., Yanagisawa, Y. and Satoh, T.: An anonymous communication technique using dummies for location-based services, *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*, IEEE, pp. 88–97 (2005).

[4] Ardagna, C. A., Cremonini, M., Damiani, E., Di Vimercati, S. D. C. and Samarati, P.: Location privacy protection through obfuscation-based techniques, *Data and Applications Security XXI*, Springer, pp. 47–60 (2007).

[5] Shokri, R., Freudiger, J. and Hubaux, J.-P.: A unified framework for location privacy, Technical report (2010).

[6] Krumm, J.: Inference attacks on location tracks, *Pervasive Computing*, Springer, pp. 127–143 (2007).

[7] Ying, J. J.-C., Lee, W.-C., Weng, T.-C. and Tseng, V. S.: Semantic trajectory mining for location prediction, *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, ACM, pp. 34–43 (2011).

[8] Isaacman, S., Becker, R., Cáceres, R., Kobourov, S., Martonosi, M., Rowland, J. and Varshavsky, A.: Identifying important places in people's lives from cellular network data, *Pervasive computing*, Springer, pp. 133–151 (2011).

[9] Arai, A., Witayangkurn, A., Horanont, T., Shao, X. and Shibasaki, R.: Understanding the Unobservable Population in Call Detail Records through Analysis of Mobile Phone User Calling Behavior, *Pervasive Computing and Communications (PerCom), 2015, IEEE International Conference on*, IEEE, pp. 207–214 (2015).

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

[11] Shokri, R., Theodorakopoulos, G., Danezis, G., Hubaux, J.-P. and Le Boudec, J.-Y.: Quantifying location privacy: the case of sporadic location exposure, *Privacy Enhancing Technologies*, Springer, pp. 57–76 (2011).

[12] Shokri, R., Bindschaedler, V., Theodorakopoulos, G., Danezis, G., Hubaux, J.-P. and Le Boudec, J.-Y.: Location-Privacy Meter: A Tool to Quantify Location Privacy, `http://lca.epfl.ch/projects/quantifyingprivacy/` (2011).

[13] Sekimoto, Y., Shibasaki, R., Kanasugi, H., Usui, T. and Shimazaki, Y.: Pflow: Reconstructing people flow recycling large-scale social survey data, *IEEE Pervasive Computing*, Vol. 10, No. 4, pp. 0027–35 (2011).