様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　５　月　　７　日現在

機関番号：　１４４０１
研究種目：　挑戦的萌芽研究
研究期間：　2016～2017
課題番号：　１６Ｋ１２４２９

研究課題名（和文）位置情報サービス利用における位置プライバシー保護技術の実用性向上

研究課題名（英文）Improving Practicality of Location Privacy Preserving Techniques for Location-based Service Usage

研究代表者

原　隆浩（Hara, Takahiro）

大阪大学・情報科学研究科・教授

研究者番号：２０２９４０４３

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：本研究では、位置情報サービス利用時に、ダミーの位置情報を用いてユーザの位置を曖昧化する手法を対象とし、従来のアプローチと比較してより実用性を重視した研究開発を実施した。具体的には、訪問場所に関するユーザの嗜好を考慮してダミーを生成する手法、および、ユーザによる移動プランに関する事前入力が訪問場所のみである場合にダミーを生成する手法として、実用性の高い技術を考案した。

研究成果の概要（英文）：In this project, we have conducted a practical research on user location anonymization using dummy locations in location-based service usage. Specifically, we have proposed a dummy generation method based on user preferences on visiting locations, and also proposed a method which requires users to input only a set of visiting locations in advance. These methods are more practical than other existing approaches.

研究分野：　データ工学

キーワード：　地理情報システム　位置プライバシー

１．研究開始当初の背景

近年、スマートフォンの爆発的な普及と無線通信の高速化に伴い、モバイルユーザに周辺の観光地やショップ、レストランなどの情報（位置依存情報）を提供する位置情報サービスが注目され、既に多くのサービスが運用されている。その一方で、位置情報サービスでは、ユーザが自身の位置をサービス提供者に通知しなければならないため、情報の不正利用や情報流出により、ユーザの現在位置や過去の移動履歴といったプライバシー（位置プライバシー[1]）が侵害されるという脅威が指摘され、最近、位置プライバシー保護に関する研究が盛んに行われている。

最初期の研究では、ユーザの移動特性として非常にシンプルで非現実的なもの（ランダムなど）を想定していたため、最近ではより現実的な想定およびアプローチの手法が提案されている。しかし、(1)ユーザの訪問場所に関する嗜好を十分に考慮してない、(2)サービス利用前にユーザが移動プラン（訪問場所、到着・滞在時間など）を入力する必要がある、など依然として実用性の面で問題が残されていた。そこで研究代表者は、安全に位置情報サービスを利用するためには、位置プライバシー保護技術の実現性のさらに高める必要があると考え、本研究を着想した。

２．研究の目的

本研究では、ユーザが位置情報サービスを継続的に利用する状況において、位置プライバシー保護のために複数のダミーの位置情報を生成する実用的な手法を考案する。具体的には、上記の問題(1)に対応するために、ユーザの嗜好の近いダミーを生成したり、逆に、ユーザとかけはなれたダミーを生成したりするなどを調整可能な手法について検討する。さらに、問題(2)に対応するために、ユーザによる事前入力の手間を軽減したうえで、位置プライバシーを十分に保護できる手法について検討する。例えば、訪問場所のみをユーザが指定したりする場合でも、ダミーを暫定的に生成し、ユーザの実際の移動状況に基づいて適応的にダミーの移動パターンを変更する手法などを考案する。

考案手法の有効性を、シミュレーション実験および被験者実験により、統計量と視認性の両方の観点から評価し、考案手法がユーザの位置プライバシーを十分に保護できることを示す。

３．研究の方法

３．１．位置プライバシー保護の要求事項

ユーザが連続的に位置情報を送信するサービスを利用する状況において、ユーザの位置プライバシーを保護するためには、以下の２つの要求を満たす必要がある。

- **追跡可能性**
  連続的に位置情報サービスを利用する場合、ユーザが一度特定されると、その前後にサービスを要求した場所まで推測され、軌跡が追跡されてしまう。
  これを防ぐためには、ユーザとダミーの移動軌跡を、直前の位置から移動可能な範囲内で交差させることが有効である。
- **匿名領域**
  ユーザとダミーを包含する凸包領域を匿名領域と呼ぶ。この領域が大きいほどユーザの位置を曖昧化できるため、ダミーは広範囲に配置させる必要がある。

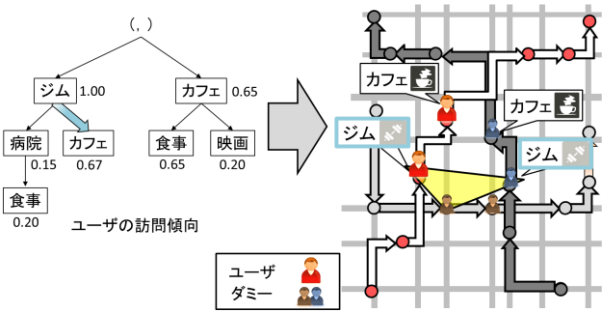


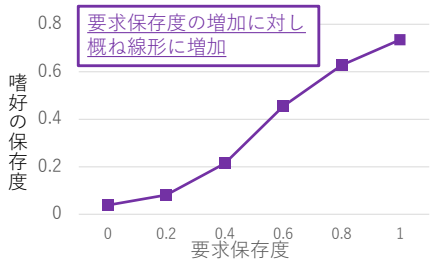
図１：ユーザの嗜好を考慮したダミー生成

３．２．ユーザの嗜好を考慮したダミー生成

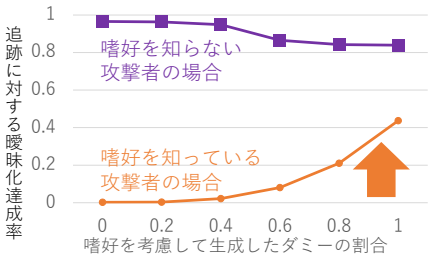
これまでのダミー生成手法では、ダミーを生成する際にユーザの嗜好が考慮されていないため、ユーザの嗜好と異なる遷移傾向を示すダミーが生成されてしまう。これは、プライバシーの観点から嗜好を保護したいユーザにとっては望ましい性質であるが、嗜好を公開することでパーソナライズされたサービスを受けたいユーザにとっては、サービスの質の低下を招く要因となる。そこで本研究では、ユーザの位置プライバシーを保護しつつ、嗜好情報についてパーソナライズとプライバシーのトレードオフを制御可能にするため、嗜好の保存度をユーザの要求に応じて制御可能なダミー生成手法を検討した。

本研究では、図１に示すように、ユーザの嗜好を訪問場所の遷移確率などとして定義可能な嗜好モデルを考案し、そのモデルとユーザが指定する嗜好依存度合に基づいて、ダミーを生成する手法を考案した。この際、３．１で説明した要求事項以外に、以下の要求を満たすことを目指した。

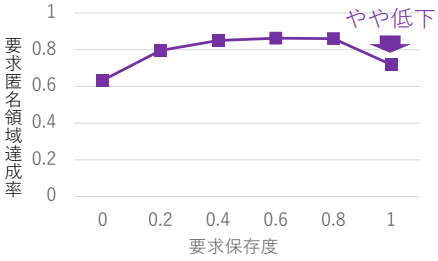
- **嗜好の保存**
  ダミーを用いた手法では、サービスプロバイダが観測できる情報は、ユーザとダミーが混在した位置情報系列となる。そのため、ダミーがユーザの嗜好と異なる動作をしている場合、ユーザ本来の嗜好におけるシーケンスの発生率と、観測される嗜好におけるシーケンスの発生率には誤差が生じる。嗜好の保存度は、この２つの嗜好の類似性を表す指標であり、これらの嗜好に含まれる全てのシーケンスにおいて発生率が完全に一致している場合に１ となる。



(a) 嗜好の保存度



(b) 追跡への曖昧化達成率



(c) 匿名領域達成率

図 2：評価結果 1

考案手法では、ユーザの嗜好に従って移動するダミーと、ユーザの嗜好と異なる動きをするダミーを、ユーザの要求する嗜好の保存度に応じた比率で生成することで、嗜好の保存度を制御する。

提案手法の有効性を評価するために、東京 23 区の地図上でユーザのサービス利用を再現し、シミュレーション評価を行った。評価では、嗜好の要求保存度の変化に対する嗜好の保存度(図 2(a))、追跡に対する曖昧化達成率(図 2(b))、匿名領域達成率(図 2(c)) の変化を調べた。図 2(a)より、嗜好の保存度が要求保存度に対し概ね線形に変化することがわかる。このことから、提案手法が要求応じて嗜好の保存度を制御可能であることを確認した。図 2(b)より、提案手法では、ユーザの嗜好を考慮してユーザらしいダミーを生成することで、嗜好を知っている攻撃者に対しても、効果的に追跡可能性を低下できることを確認した。図 2(c) より、提案手法では、全てのダミーをユーザの嗜好に従って生成した場合に要求匿名領域達成率に低下が見られた。このことから、実環境では地理的要因の影響が大きく、カテゴリシーケンスの制約と匿名領域の要求を同時に満たせる経路を発見することが困難であることがわかった。

3．3．訪問場所のみを指定する場合のダミー生成

これまでのダミー生成手法では、ユーザが事前に訪問場所・順序、滞在時間などの詳細な行動プランをシステムに入力する必要があり、実用性の面で問題があった。そこで本研究では、ユーザが訪問場所の集合のみを指定し、システム側でユーザの現在状況に基づいて柔軟かつ動的にダミーを逐次生成する手法について研究開発を推進した。

本研究では、まず準備的な手法として、推定したユーザの行動プランに基づいて既存のダミー生成手法を適用し、実際のユーザの移動状況に応じてダミーの行動プランを修正する手法を考案した。しかし、この手法は、一度生成した行動プランをなるべく保全するように修正を行うため、推定と実際の行動プランの差異が大きいと、十分に位置を曖昧化できなかった。

そこで本研究では、以下の 2 つのアプローチに基づく新たな手法 Edge を考案した。

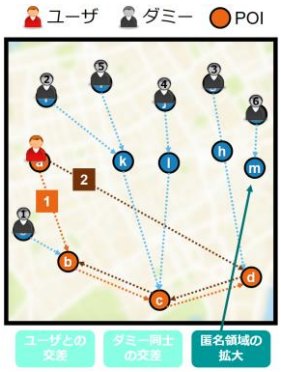
1. ユーザの移動先を複数推定する。
2. 推定した複数の移動先に基づいて、ダミーの行動プランの一部を生成する。

このようなアプローチを用いることで、ユーザの行動プランに関する特定の予測に依存することなく、ユーザの実行動に応じて柔軟にダミーを逐次生成することが可能となる。

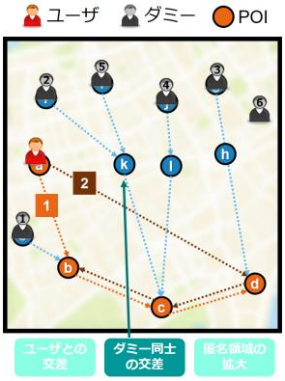
具体的には、Edge ではまず、各移動先候補の連続する 2 つの訪問場所でユーザの移動軌跡と交差するように、ダミーの行動プランを生成する(図 3(a))。これにより、ユーザとの交差が発生する間隔が短くなり、効果的に追跡可能性を低下できる。次に、ユーザだけが交差することにより、ユーザが特定されることを防ぐため、他のダミーの移動軌跡と交差を行うダミーの行動プランを生成する(図 3(b))。そして、ユーザが要求する匿名領域を満たせるように、匿名領域の拡大を行うダミーの行動プランを生成する(図 3(c))。この操作をユーザが訪問場所に到着する度に行い、ダミーの行動プランを逐次的に生成する。

提案手法の性能を検証するために、シミュレーションによる評価実験を行った。東京 23 区の地図上でユーザのサービス利用をシミュレートした実験を行った。評価指標には、追跡可能性の指標であるユーザの移動軌跡の追跡可能時間、および匿名領域の指標であるユーザの要求する匿名領域に対して実際に確保できた領域の大きさの割合である匿名領域達成率を用いた。図 4(a)は、ダミーの数に対する評価指標の変化を示している。この結果より、Edge は追跡可能時間を最も小さくできており、十分に追跡可能性を低下できることを確認した。図 4(b)より、Edge の匿名領域達成率は 1.0 程度あり、ユーザが要求する匿名領域を確保できることも確認した。

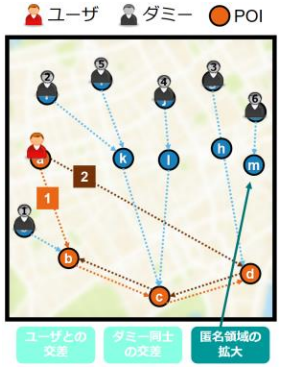
さらに目視によるユーザ識別に対する頑強性を調査するため、視認性実験を行った。この実験には、大学院生 23 名が参加し、ダ



(a) ユーザとの交差



(b) ダミー同士の交差



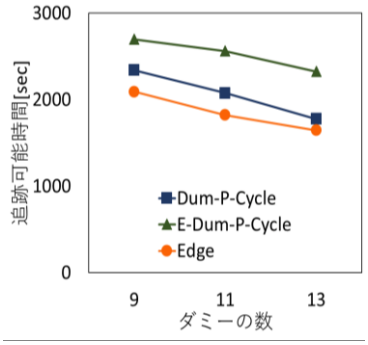
(c) 匿名領域の拡大

図 3：逐次的ダミー生成手法

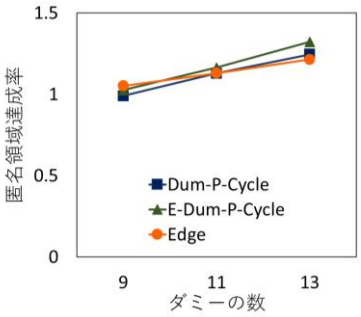
ミーの中からユーザの判別する実験を 1,078 回、ユーザの位置を一旦暴露した後にどのくらいの時間で曖昧化できるかを調べる追跡実験を 2,335 回実施した。その結果、ユーザの判別性、追跡性ともに十分小さいことを確認した。

4．研究成果

本研究では、位置情報サービス利用時に、ダミーの位置情報を用いてユーザの位置を曖昧化する手法を対象とし、従来のアプローチと比較してより実用性を重視した研究開発を実施した。具体的には、訪問場所に関するユーザの嗜好を考慮してダミーを生成する手法、および、ユーザによる移動プランに関する事前入力が訪問場所のみである場合にダミーを生成する手法として、実用性の高い技術を考案した。



(a) 追跡可能時間



(b) 匿名領域達成率

図 4：評価結果 2

本研究の成果は、5 で示すように、著名な国際論文誌である IEEE Access に採択されており、さらに国内学会において 3 件の研究発表を行っている。また、国際ワークショップにおいて、本研究の成果に関して基調講演を行っている。これらの実績は、本研究の成果が国際的に高く評価されていることを示している。

以上のことから、本研究は挑戦的萌芽研究として、十分な成果を達成したものと考える。

5．主な発表論文等

〔雑誌論文〕（計　1　件）

① Shuhei Hayashida, Daichi Amagata, Takahiro Hara, Xing Xie, Dummy Generation Based on User-Movement Estimation for Location Privacy Protection, IEEE Access, 掲載決定, 2018.

〔学会発表〕（計　3　件）

① 林田 秀平, 水野 聖也, 天方 大地, 原 隆浩, Xing Xie, ユーザの移動状況に適応したダミーによる位置曖昧化手法, 情報処理学会マルチメディア, 分散, 協調とモバイル(DICOMO2016)シンポジウム, 2016 年 7 月.

② 林田 秀平, 天方 大地, 原 隆浩, Xing Xie, ユーザの移動先候補の推定に基づく逐次的なダミー生成による位置曖昧化手法, 情報処理学会マルチメディア, 分散, 協調とモバイル(DICOMO2017)シン

ポジウム, 2017年7月.
③ 林田 秀平,天方 大地, 原 隆浩, Xing Xie,位置情報サービス利用におけるダミーを用いたユーザ位置曖昧化手法の視認性評価, データ工学と情報マネジメントに関するフォーラム(DEIM2018), 2018年3月.

〔図書〕(計 0 件)

〔産業財産権〕

○出願状況(計 0 件)
○取得状況(計 0 件)

〔その他〕
基調講演 : Takahiro Hara, Dummy-based Approaches for Protecting Location Privacy, Central Area Networking and Security Workshop (CANSec 2017), Missouri University of Science and Technology, Rolla, MO, USA, October 28, 2017.

６．研究組織

(1)研究代表者
原 隆浩 (HARA, Takahiro)
大阪大学・大学院情報科学研究科・教授
研究者番号：２０２９４０４３

(2)研究協力者
Xing XIE
マイクロソフト研究所(中国)・シニアリサーチマネージャ

Christian S. JENSEN
オールボー大学(デンマーク)・教授