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

令和　元 年　 ５ 月 １７ 日現在

機関番号：８２６２６
研究種目：若手研究(B)
研究期間：2016～2018
課題番号：１６Ｋ１６０６９

研究課題名（和文）信頼できる機関を仮定しない空間統計データ構築技術の開発

研究課題名（英文）Privacy Preserving Population Distribution Estimation without Trusted Third Parties

研究代表者
村上　隆夫（Murakami, Takao）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：８０５８７９８１

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では，ユーザが自分自身で位置情報に（ノイズを加える等の）加工を施した上でサービス提供事業者に送信し，サービス提供事業者が大量の加工済み位置情報を元に空間統計データを構築する「空間統計データ構築技術」の確立に向けて，精度と安全性の両面から研究成果を上げた．まず，分布推定法として最も有望な従来手法である反復ベイズ法の分布推定誤差を低減する手法を提案し，理論と実験の両面から高精度化が可能であることを示した．次に，従来の加工メカニズムの匿名性という観点から安全性を詳細に解析し，OptSQLメカニズムが匿名性の観点で優れていることを示した．

研究成果の学術的意義や社会的意義
従来の空間統計データ構築技術は，サービス提供事業者が信頼できる機関（TTP: Trusted Third Party）であると仮定しているが，情報漏洩の事故が多発している近年ではこの仮定が成立しなくなってきている．従って，本研究での成果は，ユーザにプライバシーの観点で真の安心感を与えるという大きな意義を持つ．また，その結果，より多くのユーザから大規模な位置情報を収集することが可能となるため，従来よりも高精度な空間統計データの構築も可能となる．

研究成果の概要（英文）：In this work, we studied privacy preserving population distribution estimation without trusted third parties, in which users obfuscates their locations by themselves and a data collector estimates population distribution statistics based on obfuscated location data. We first focused on the iterative Bayesian method, which is a state-of-the-art distribution estimation method, and proposed a method to reduce its estimation error. We showed, both theoretically and experimentally, that the estimation accuracy is improved. We then analyzed the security of the existing obfuscation mechanisms in terms of anonymity, and showed that OptSQL has promising in terms of the capability of anonymization.

研究分野：プライバシー保護

キーワード：位置情報プライバシー　空間統計データ　TTP　加工メカニズム　分布推定

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年，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，データセンターやクラウドに蓄積された大多数のユーザの位置情報（位置情報ビッグデータ）を利活用したサービスが注目されている．その代表的なサービスとして，人口分布や交通量分布などの「空間統計データ」を企業・自治体や一般個人に提供するサービスがある．このようなサービスは観光振興，防災，経路案内など様々な用途で活用される一方で，ユーザのプライバシーが侵害される恐れがある．例えば，空間統計データからユーザと場所のペアを特定することで，ユーザの自宅や通院している病院などが推測される恐れがある．また，SNS 上で公開された位置情報を利用した空き巣事件や，GPS の位置情報を基にしたストーカー事件なども，実際に起きている．

これに対して従来，空間統計データに対して（人数値にノイズを加える等の）加工を施す技術が幅広く研究されている．その多くは，Dwork（文献①）によって提案された「差分プライバシー」（Differential Privacy）と呼ばれる安全性基準に基づくものである（文献②③④）．差分プライバシーは「ある人がデータベースに含まれているか否かの判別困難性」を安全性の根拠とする基準であり，これらの手法は「どのような背景知識を持った攻撃者が加工後のデータを入手したとしても，ユーザと場所のペアに関する情報を新たに得ることができない」という安全性を保証する．

しかし，情報漏洩の事故が多発している近年においては，ユーザがサービス提供事業者を完全に信頼することが困難になってきている．具体的な事例として，2015 年 5 月に日本年金機構が標的型メールによる攻撃を受け，約 125 万件の氏名と基礎年金番号などの個人情報が漏洩する事故が起きている．こうした状況において，サービス提供事業者が収集した（加工前の）全ユーザの位置情報が漏洩する（その結果，全ユーザのプライバシーが侵害される）という極めて深刻な事故へのユーザの不安を払拭することはできない．

２．研究の目的

本研究では，信頼できる機関（TTP: Trusted Third Party）を一切仮定しない「空間統計データ構築技術」を確立する．これは，(1) ユーザが自分自身で位置情報に（ノイズを加える等の）加工を施した上でサービス提供事業者に送信し，(2) サービス提供事業者が大量の加工済み位置情報を元に空間統計データを構築するものである．個々の加工済み位置情報からは，正確な位置を知ることができない．これにより大量の位置情報の漏洩という根本的な問題を解決し，ユーザにプライバシーの観点で真の安心感を与える空間統計データの構築技術を目指す．

３．研究の方法

TTP 不要な空間統計データ技術は，各ユーザの位置情報に加工を施す「加工メカニズム」と大量の加工済み位置情報から，空間統計データを構築する（加工前の位置情報の分布を推定する）「分布推定法」に分けることができる．前者については，k-ary randomized response（文献⑤），二次元ラプラスメカニズム（文献⑥）などが従来手法として提案されており，後者については逆行列法や反復ベイズ法（Expectation-Maximization reconstruction 法）（文献⑦）などが提案されている．

本研究では，TTP 不要な空間統計データ技術の確立に向けて，以下の 2 つのステップに分けて研究を進める．(1) まず，高精度な空間統計データ技術を確立するため，加工メカニズムとしては従来手法（k-ary randomized response など）を用い，分布推定法を高精度化する検討を行う．より具体的には，分布推定法として最も有望な従来手法である反復ベイズ法に着眼し，その分布推定誤差を低減するアプローチを検討する．(2) 次に，安全性の高い空間統計データ技術を確立するため，従来の加工メカニズムの安全性を詳細に解析する．より具体的には，従来の加工メカニズムは「位置情報の曖昧化」に関する安全性指標を満たすものとして提案されているが（例えば，k-ary randomized response は差分プライバシーを満たし，二次元ラプラスメカニズムはその変形版である Geo-indistiguishability を満たす），その加工メカニズムによって加工されたデータが持つ「匿名性」の性質については十分に議論がされていない．そこで，加工データが持つ匿名性を解析する．また，位置データの再識別リスクを明確にするため，新たな再識別攻撃法を確立し，再識別リスクを評価する．

４．研究成果

平成 28 年度および平成 29 年度では，高精度な空間統計データ技術の確立に向けた研究を行った．具体的には，加工メカニズムとしては randomized response を用い，反復ベイズ法の分布推定誤差を低減する手法を開発した．反復ベイズ法は，EM（Expectation Maximization）アルゴリズムに基づいて，加工前の位置サンプルの分布を推定する手法であり，サンプル数に依存せずに最尤推定と等価であることが知られている（逆行列法もサンプル数が十分大きいときに最尤推定となるが，小さいときは最尤推定とならず，非常に精度が悪い）．しかし，最尤推定はサンプル数が小さいときに分布推定誤差が大きいことが知られている．

そこで，平成 28 年度および平成 29 年度では，反復ベイズ法の有限サンプルにおける分布推定誤差を，Rilstone らの理論に基づいて補正する手法を確立した．この手法では，まず Rilstone らの理論に基づき，反復ベイズ法の有限サンプルにおける分布推定誤差を推定する．その際，フィッシャー情報行列の逆行列を推定する必要があるが，ユーザ数や privacy budget（局所型

差分プライバシーのパラメータ）が小さいときに，この逆行列の推定値が正確でないという課題がある．この課題を解決するため，分布推定誤差を推定した後，重み係数をかけた上で，反復ベイズ法の推定値から差し引く手法を提案した．この重み係数は，パラメトリック・ブートストラップ法のように，経験分布から人工データを生成し，その人工データに基づくシミュレーションによって最適化した．尚，Rilstone らの理論は元々二次バイアス（second-order bias）を推定するための理論であるが，提案手法によって二次 MSE（second-order Mean Square Error）を 0 に減らせることを，幾つかの仮定の下で理論的に証明した．

提案手法の有効性を示すために，2 つの位置情報データセットと 1 つの国勢調査のデータセットの計 3 つの実データを用いた評価実験を行った．その結果，提案手法が反復ベイズ法と比べて大幅な精度向上が可能であることを，全てのデータセットで示した．本成果は，プライバシーのトップ国際会議兼国際誌である PETS/PoPETs 2018 に採択された（雑誌論文①）．また，PWS 勉強会（PWS Seminar 2018）にて本内容に関する招待講演を行った（学会発表③）．

平成 30 年度では，安全性の高い空間統計データ技術の確立に向けた研究を行った．具体的には，加工メカニズムの state-of-the-art である二次元ラプラスメカニズム（文献⑥）と Optimal Geo-indistinguishability (OptQL) メカニズム（文献⑧）が持つ匿名性を解析した．二次元ラプラスメカニズムと OptQL メカニズムは共に，差分プライバシーに元データと加工データとのユークリッド距離という「距離尺度」の概念を導入した Geo-indistiguishability（文献⑥）を満たすもので，「大まかな位置（例：東京に住んでいるという事実）の漏洩は許すが，正確な位置（例：具体的な住所）は漏洩しない」というような安全性の性質を持つ．（尚，OptQL は Geo-indistiguishability を満たすメカニズムの中で，元データと加工データのユークリッド距離の期待値が最小である，という特徴を持つ．）しかし，Geo-indistiguishability は位置情報の曖昧化に関する安全性指標であり，二次元ラプラスメカニズムと OptQL メカニズムの匿名性の性質については明らかになっていない．例えば，サービス事業者がユーザから加工データを収集した後，別の事業者に第三者提供するような場合，再識別ができないように（即ち，匿名性を満たすように）加工データを匿名加工することが重要である．

そこで，二次元ラプラスメカニズムと OptQL メカニズムが持つ匿名性を評価した．具体的には，メカニズムが持つ匿名性に関する性質として，データベースに対する匿名性の指標である k-匿名性を一般化した，κ-asymptotic anonymity を定義した．これは入力分布πとメカニズム Q のペア(π,Q)が与えられたときに，出力確率 $p(x)$が $p(x) > 0$ となるあらゆる出力値 x に対して $p(x) > \kappa$が成立する，という定義であり，(π,Q)がκ-asymptotic anonymity を満たすとき，加工データが k-匿名性を実現するのに必要なユーザ数はおよそ k/κとなる．実験的に二次元ラプラスメカニズムと OptQL メカニズムのκ-asymptotic anonymity を評価し，OptQL の方がκ-asymptotic anonymity の観点で優れている，即ち匿名性を達成しやすいことを示した．本成果は，国際会議 ISITA2018 で発表した（学会発表①）．

また，位置データの再識別リスクを明確にするため，新しい再識別攻撃法に関する研究も行った．サービス事業者が，ユーザのトレース（移動履歴）に対して仮名化のみを施した上で，別の事業者に第三者提供する場合を考える．この場合，仮名化トレースに対する再識別攻撃を行うアプローチとして，テンソル分解に基づく再識別攻撃が，少量の学習用データで特に有効なアプローチとして知られている（文献⑨）．しかし，この攻撃法はユーザの遷移パターンをモデル化するもので，攻撃者がターゲットとするユーザに対して 1 個の位置情報しか学習用データとして得られなかった場合には適用できないなど，改善の余地があった．

そこで，ユーザの遷移パターンではなく，各位置に対する滞在確率をモデル化する新たな再識別攻撃を提案した．提案手法では，まず学習用データを基に，各ユーザ・各位置の滞在確率で構成される行列を行列分解により推定する．その後，仮名化トレースから得られる滞在分布と各ユーザの滞在分布との JS（Jensen-Shannon）divergence を求め，その最も小さいユーザのものとして識別する．実データを用いた評価実験の結果，学習データが少量のときに，提案手法が，テンソル分解に基づく再識別法よりも高い再識別率を実現できることを示した．本攻撃法に対する対策としては，例えば上述したように，ユーザが自身のトレースに対して OptQL を用いて加工し，その後，サービス事業者が匿名性（k-匿名性など）を満たすように匿名加工する，などの対策が考えられる．本成果は，国際会議 ISITA2018 で発表した（学会発表②）．

＜引用文献＞

① C.Dwork, “Differential Privacy,” Proceedings of International Colloquium on Automata, Languages, and Programming (ICALP’06), pp.1-12, 2006.

② B.Barak, K.Chaudhuri, C.Dwork, S.Kale, F.McSherry, K.Talwar, “Privacy, Accuracy, and Consistency Too: A Holistic Solution to Contingency Table Release,” Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems (PODS’07), pp.273-282, 2007.

③ X.Xiao, G.Wang, J.Gehrke, “Differential Privacy via Wavelet Transforms,” IEEE Transactions on Knowledge and Data Engineering, vol.23, no.8, 2011.

④ G.Cormode, C.Procopiuc, D.Srivastava, T.T.L.Tran, “Differentially Private Summaries for Sparse Data,” Proceedings of the 15th International Conference on Database Theory (ICDT’12), pp.299-311, 2012.

⑤ P.Kairouz, K.Bonawitz, D.Ramage, “Discrete Distribution Estimation under Local Privacy,” Proceedings of the 33 rd International Conference on Machine Learning (ICML’16), pp.2436-2444, 2016.
⑥ M.E.Andres,N.E.Bordenabe,K.Chatzikokolakis,C.Palamidessi,“Geo-indistinguishability: Differential Privacy for Location-based Systems,” Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS’13), pp.901-914, 2013.
⑦ R. Agrawal, R. Srikant, D. Thomas, “Privacy Preserving OLAP,” Proceedings of the 2005 ACM SIGMOD international conference on Management of data (SIGMOD’05), pp.251-262, 2005.
⑧ N.E.Bordenabe, K.Chatzikokolakis, C.Palamidessi, “Optimal Geo-Indistinguishable Mechanisms for Location Privacy,” Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS’14), pp.251-262, 2014.
⑨ T. Murakami, H. Watanabe, “Localization Attacks Using Matrix and Tensor Factorization,” IEEE Transactions on Information Forensics and Security, Vol.11, No.8, pp.1647-1660, 2016.

５．主な発表論文等

〔雑誌論文〕（計 1 件）

① Takao Murakami, Hideitsu Hino, Jun Sakuma,“Toward Distribution Estimation under Local Differential Privacy with Small Samples,”Proceedings on Privacy Enhancing Technologies (PoPETs), Issue 3, pp.84-104, 2018.

〔学会発表〕（計 3 件）

① Yusuke Kawamoto, Takao Murakami,“On the Anonymization of Differentially Private Location Obfuscation,”Proceedings of the 2018 International Symposium on Information Theory and Its Applications (ISITA 2018), pp.159-163, 2018.
② Takao Murakami,“A Succinct Model for Re-identification of Mobility Traces Based on Small Training Data,”Proceedings of the 2018 International Symposium on Information Theory and Its Applications (ISITA 2018), pp.164-168, 2018.
③ 村上隆夫,“**局所型差分プライバシーと分布推定への応用**”, PWS **勉強会**（PWS Seminar 2018）, 2018.