科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１８　日現在

機関番号：　８２６５７
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５００１０７

研究課題名（和文）推論攻撃を考慮した位置情報プライバシー保護技術の研究

研究課題名（英文）Study on location privacy against inference attacks

研究代表者
南　和宏（Minami, Kazuhiro）

大学共同利用機関法人情報・システム研究機構（新領域融合研究センター及びライフサイ・新領域融合研究センター・特任准教授

研究者番号：１０５７９４１０

交付決定額（研究期間全体）：（直接経費）　　3,800,000円、（間接経費）　　1,140,000円

研究成果の概要（和文）：近年、インターネット上で様々な位置情報サービスが提供されており、位置情報の共有が進んでいる。しかし位置情報は我々のプライバシーに関する行動と深く関係するため、位置情報の公開は適切に制限される必要がある。しかし我々の移動パターンは多くの場合に類推可能であるため、公開した位置情報から秘密にしたい非公開の位置情報を推測されることを適切に防ぐ新しいアクセス制御の方法を考案し、その有効性を実証的に評価した。

研究成果の概要（英文）：The rise of location-sharing services on a number of mobile platforms have recently opened up the possibilities of sharing location information with other users. However, location sharing raises significant privacy concerns because location data (e.g., visiting a hospital) can be used to infer a user's personal activities. Since it is often possible to infer a user's suppressed location data from disclosed public locations considering strong spatial and temporal correlation among them, we develop a new access-control scheme against such inference attacks and conduct experiments with a real location dataset to show the effectiveness of our proposed method.

研究分野：　情報学

科研費の分科・細目：　ソフトウエア

キーワード：　位置情報プライバシー　プライバシー保護　匿名化　アクセス制御　マルコフ連鎖

１．研究開始当初の背景

最近、インターネット上では様々な位置情報サービスが提供されており、多数のユーザー間での位置情報の共有が実現されている。しかし位置情報はユーザーのプライバシーに関する行動に深く関連するため、位置情報の公開及び２次利用は適切に制限される必要がある。

しかし、位置情報データには２つの特徴があり、既存のプライバシー保護技術では十分ユーザーのプライバシーを保護できない。一つは位置情報データに時空間の強い相関性が存在する点である。したがってデータ間の相関性を考慮することで公開された位置情報から非公開のデータを推論される危険性が高い。２つめは、ユーザーの位置情報に関する外部知識が、物理的な目撃または住所録といった別の情報ソースから容易に入手可能な点である。そのような外部知識を利用して匿名化されたデータからユーザーを再識別することが可能な場合もある。

このように上記２つの問題に対処するプライバシー保護技術、特にアクセス制御と匿名化、に関する新規技術の確立が望まれていた。

２．研究の目的

位置情報データ間の相関性及び外部知識の取得の容易性を考慮し、代表的プライバシー保護技術である (1) アクセス制御と (2) 匿名化に関する新規技術を確立する。(1)においては、位置情報の時空間の相関性の問題への対処方法、(2)では外部知識による匿名化データの再識別化リスクの低減方法を主な研究課題とした。

(1)のアクセス制御に関する具体的研究目標は、①時系列の位置情報の確率的モデル化、②間接的な情報漏洩を考慮したプライバシー要件の定義、③確率的移動モデルを用いた推論攻撃に対処するアクセス制御のアルゴリズムの考案、の３つである。

(2)の匿名化に関しては、通常の匿名化技術で失われる移動軌跡の情報を保存する安全な仮名化技術の確立を目指す。具体的には、①移動の軌跡の不確定性を定量化したプライバシー指標の定式化、②外部知識による再識別化のリスクを低減する動的仮名交換手法の確立、③仮名化データの安全性評価アルゴリズムの開発、の３つを目的とする。

３．研究の方法

(1) アクセス制御は下記の手順で研究を進める。

①人々の確率的な移動パターンをマルコフ過程でモデル化し、プライバシー指標を定式化する。

②さらに「位置情報が非公開である」である事実から得られる情報を用いた非公開情報に関する推論プロセスをモデル化する。

③上記①②の推論モデルに基づく攻撃を対象とするアクセス制御アルゴリズムを設計

④実際の位置情報データを用い、提案手法の有効性を評価する。具体的な指標としては、システムが非公開と判断する位置情報の数を従来手法と本研究の新規手法で比較する。

(2)の匿名化に関しては下記の手順で研究を進める。

①動的仮名交換による位置情報データの加工技術を開発する。

②ユーザーの可能経路数に基づくプライバシー指標を定式化する。

③仮名化データの安全性を検証するアルゴリズムを考案し、その正確性、計算量の解析を行う。

④実際の位置情報データを用い、開発した安全性評価アルゴリズムのシステム性能を評価する。

４．研究成果

(1)アクセス制御に関しては、位置情報の相関性を考慮したプライバシー指標を定式化し、図１に示すマルコフ連鎖に基づくアクセス制御アルゴリズムを考案した。基本アイデアは位置情報を提供するユーザーの過去の移動履歴を学習したマルコフモデルの推論エンジンをアクセス制御システムに組み込み、そのエンジンを用いて非公開の位置情報をあるしきい値以上の確率で推論できない場合のみ、位置情報を公開する手法である。

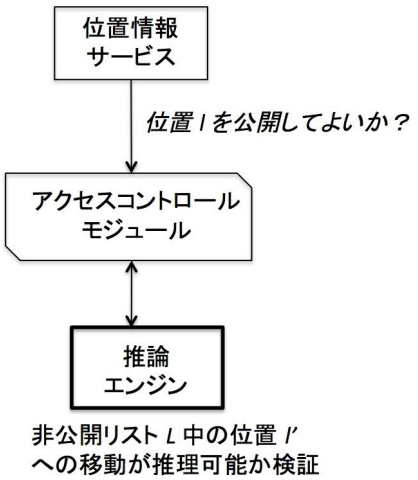

図１．推論エンジンを用いたアクセス制御

また単純なマルコフモデルでは捉えきれない「サービスから位置情報が提供されない（つまり現在位置が非公開）」という間接的な情報漏洩を用いた推論プロセスを考察し、このような推論を通常のマルコフモデルに反映させる変換アルゴリズムを考案した。

さらにマイクロソフト北京研究所が公開する位置情報データを用いて、統計的推論攻撃のリスクを定量的に評価した。図２に示す実証実験の結果は、「位置情報が非公開」である事実から機密の非公開に位置情報に関する多くの情報が入手可能であることを示した。

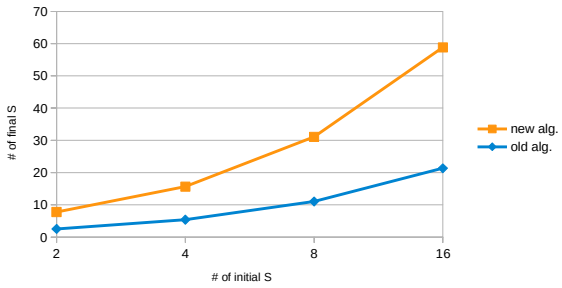

図２．初期秘匿位置の数とそれらの機密性を保つために必要な最終秘匿位置の関係．通常のマルコフ連鎖による推論と、「情報の非公開」による追加の推論の結果を比較している．

この位置情報を題材にした時系列データのアクセス制御に関する研究は機械学習とプライバシー保護技術の密接な関連性を広く認知させ、国際会議（ICMU2014）において Best Paper Award を受賞した。

(2)匿名化に関しては、図３に示す「ミックスゾーン」と呼ぶ複数のユーザーが出会う地点でランダムに仮名交換を行う新規の仮名化技術を考案した。

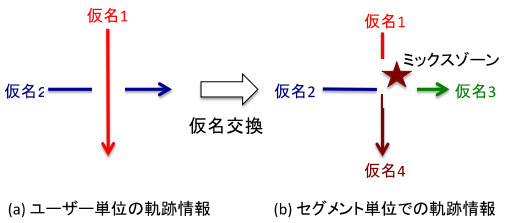

図３．ミックスゾーンにおける仮名交換

時系列軌跡の関連をミックスゾーンで分断することで、通常の仮名化処理で課題となる外部知識をもつ攻撃者が特定個人を再識別するリスクを局所化することができる。図４に示すように再識別されたユーザーは一定時間経過後に複数のミックスゾーンを経由することで到達可能な場所に関する十分な不確定性を得ることができる。

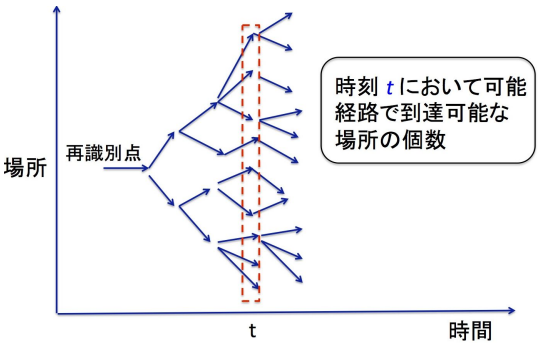

図４．代替経路に基づくプライバシー指標

このユーザーの代替可能経路に着目したプライバシ指標を定式化し、仮名化データが各ユーザーに対して十分な代替経路を確保しているか安全性を検証する効率的な多項式時間のアルゴリズムを考案した。

さらにプライバシー要件を満足する最小のミックスゾーンの組み合わせを見つける最適化アルゴリズムを実装し、現在はサンフランシスコのタクシーの運行状況に関する位置情報データから抽出したミックスゾーンのグラフ構造を抽出し、プライバシーとデータ効用のトレードオフの実証的評価を行なっている。

ビッグデータの中核は非常に疎で多次元連続的な我々の行動履歴データであり、既存の k 匿名化手法ではデータの劣化を防ぐ根本的な解決策が見当たらないのが現状である。本研究では仮名の動的交換という従来とは異なる手法で「次元の呪い」の問題を回避しつつ時系列軌跡情報の公開する可能性を提示しており、プライバシー保護データ公開技術の新たな研究領域を拓いたと言える。

５．主な発表論文等

〔雑誌論文〕（計　１件）

①南和宏．プライバシ保護データパブリッシング．情報処理．Vol.54，No.9，2013.査読有．

〔学会発表〕（計　６件）

①Tomoya Tanjo, Kazuhiro Minami, Ken Mano, and Hiroshi Maruyama. On Safety of Pseudonym-based Location Data in the Context of Constraint Satisfaction Problems. In Proceedings of the 2014 Asian Conference on Availability, Reliability and Security, April, 2014. 査読有.
② Kazuhiro Minami. Preventing Denial-of-request Inference Attacks in Location-sharing Services. In Proceedings of the 7th International Conference on Mobile Computing and Ubiquitous Networking (ICMU), January, 2014. 査読有.
③ Ken Mano, Kazuhiro Minami, and Hiroshi Maruyama. Privacy-preserving Publishing of Pseudonym-based Trajectory Location Data Set. In Proceedings of the 2nd International Workshop on Security of Mobile Applications, September, 2013. 査読有.
④ Hiroshi Maruyama, Kiyoshi Watanabe, Sachiko Yoshihama, Naohiko Uramoto, Yoichi Takehora, and Kazuhiro Minami. ICHIGAN Security - A Security Architecture that Enables Situation-Based Policy Switching. In Proceedings of the 3rd International Workshop on Resilience and IT-Risk in Social Infrastructures, September, 2013. 査読有.

⑤ Ken Mano, Kazuhiro Minami, and Hiroshi Maruyama. Protecting Location Privacy with K-Confusing Paths Based on Dynamic Pseudonyms. In Proceedings of the 5th IEEE International Workshop on SEcurity and SOCial Networking, March, 2013. 査読有.
⑥ 南和宏, 推論攻撃を考慮した論理データベースのためのアクセスコントロール, 2012 年 暗号と情報セキュリティシンポジウム（SCIS2012）, 2012 年 1 月.査読なし.

〔産業財産権〕
○出願状況（計　1 件）

名称：仮名交換型位置情報提供システム
発明者：真野健, 南和宏, 丸山宏
権利者：NTT/情報･システム研究機構
種類：特許権
番号：2012-243661
出願年月日：2012 年 11 月 5 日
国内外の別： 国内

〔その他〕
ホームページ等
http://systemsresilience.org/minami/

６．研究組織
(1)研究代表者
南　和宏（Minami, Kazuhiro）
情報･システム研究機構･特任准教授
研究者番号：10579410