位置情報プライバシーをどう守るか？

Protecting Location Privacy against Inference Attacks

南　和宏
Kazuhiro Minami

何がわかる？

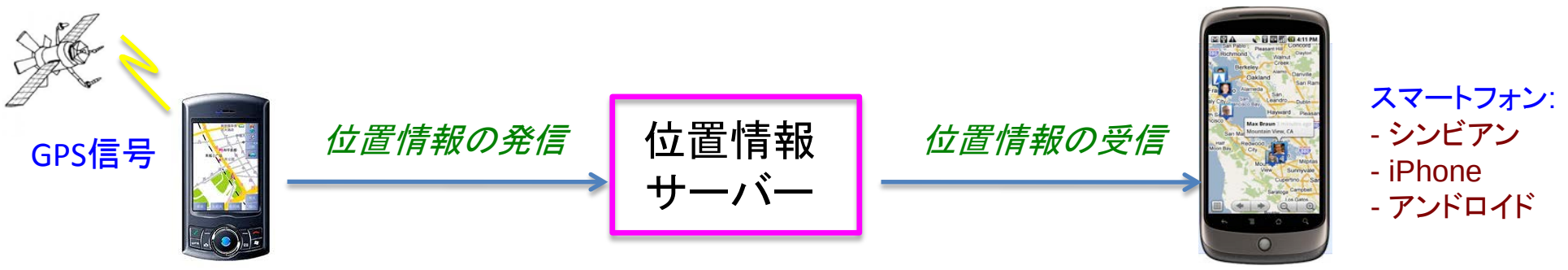
- 過去の履歴から位置情報の推論が可能であることを実証実験で検証しました。
- プライベートな位置情報を守るためには、推論エンジンを組み込んだアクセスコントロールの仕組みが有効であることを示します。

どんな研究？

- モバイルユーザーのプライバシーに関わる位置情報を適切に守るアクセス･コントロールの新しい仕組みを提案します。
- 過去の位置情報の履歴を用いた推論攻撃の危険性を定量的に評価し、それに対する防護策を講じます。

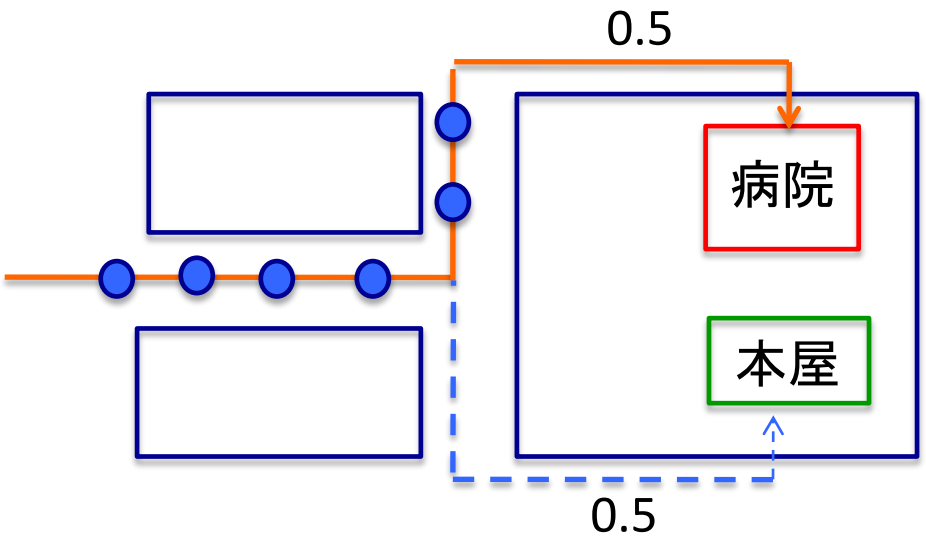
研究の背景

GPS位置情報を受信できるスマートフォーンが普及し、モバイル･ユーザーは様々な位置情報サービス（例えば、Google Latitude, Twitter Geotagging）に位置情報を発信するようになりました。しかし位置情報はプライバシーの侵害につながる危険性があります。



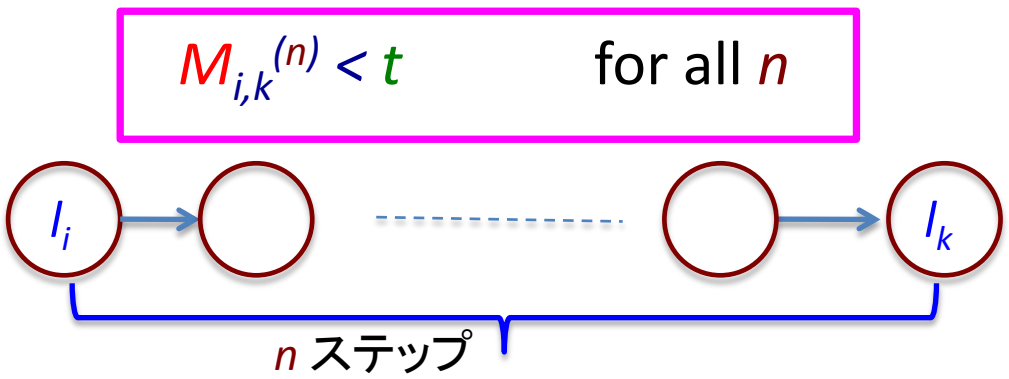
過去の移動パターンを利用した推論攻撃

突き当たりを曲がった時点で病院に行くと推論できてしまう

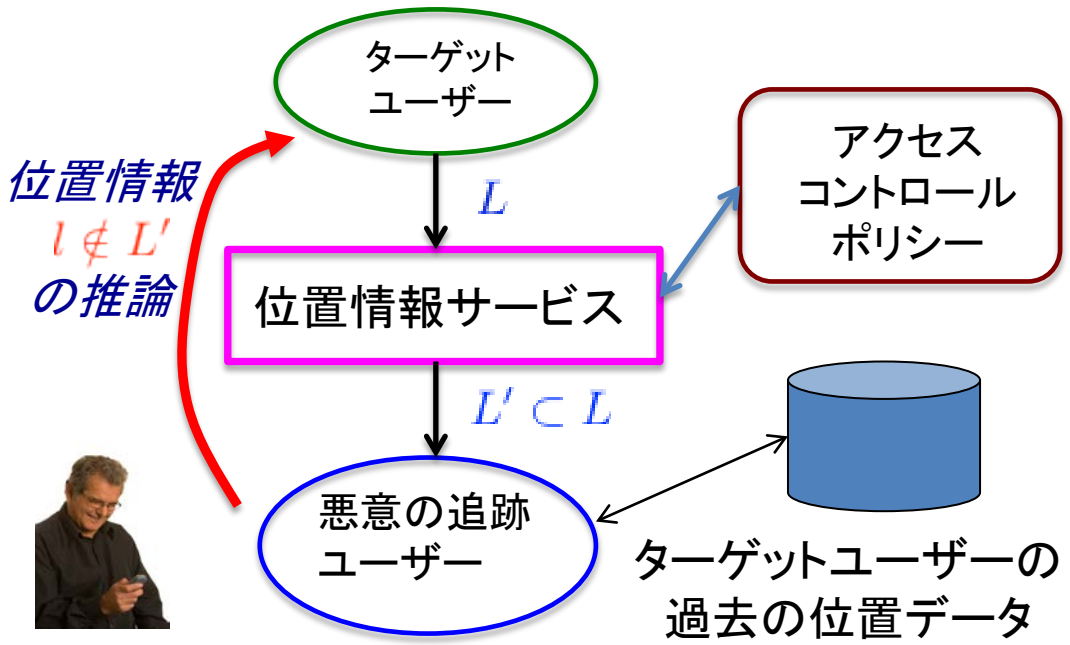


(M, t)-位置情報プライバシー

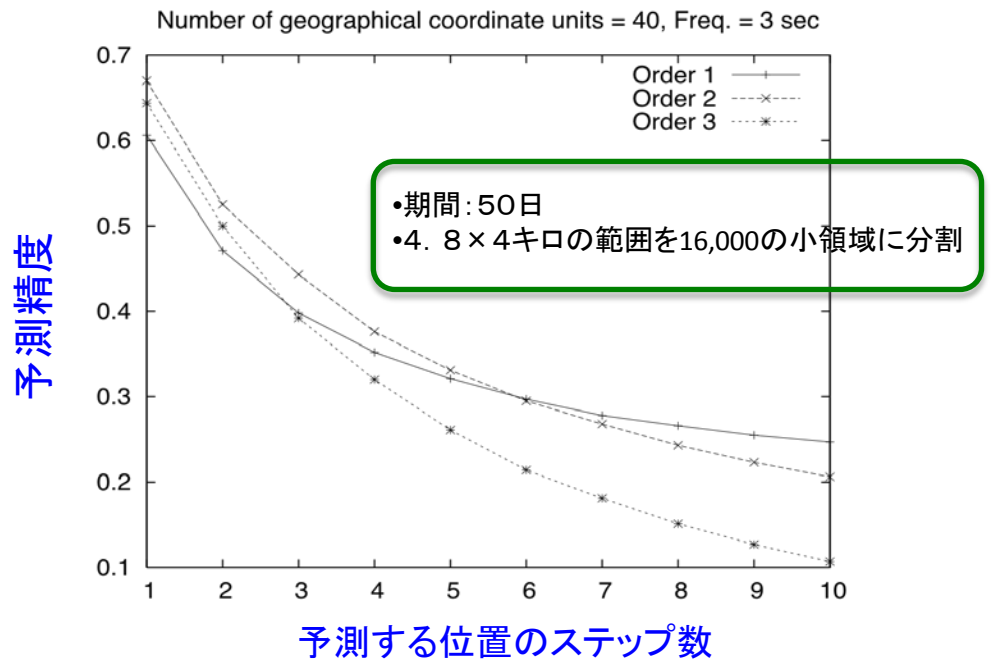
- 悪意の追跡ユーザーと2つのパラメータを考慮する
  - ターゲットユーザーの状態遷移マトリックス M
  - プライバシーしきい値 t
- 全ての位置 l_i, 全ての秘密の位置 l_k に対し、



マルコフモデルを用いた攻撃モデル



位置情報推論の実証評価



NII
連絡先：南　和宏（Kazuhiro Minami）／ 国立情報学研究所　アーキテクチャ研究系　特任准教授
TEL：03-4212-2191　　FAX：03-3556-1916　　Email：minami@nii.ac.jp