5N-7

参加型センシングにおけるプライバシー保護手法

趙 セイ † 董 ティティ † 石川 佳治 † §
† 名古屋大学情報科学研究科 § 国立情報学研究所

1 はじめに

1.1 背景

近年，多種のセンサ機能を搭載する携帯機器の普及により，ユーザの携帯機器をセンシング機器として用いる一種のクラウドソーシングである**参加型センシング**（participatory sensing）が注目されている [1]．参加型センシングでは，複数の参加者から得られるデータに基づき，交通状況などの興味のある情報を獲得することを目指している．ただし，収集されたデータから，参加者のプライバシーに関わる情報が推定される恐れがある．

現在では，位置情報に着目するプライバシー保護の研究が多くなされている [2, 4, 5]．しかし，参加型センシングにおいては，位置情報以外のプライバシーに関わる属性を用いることがあるため，位置情報以外の属性も考慮したプライバシー保護手法の開発が必要となる．

1.2 属性情報の利用と匿名化

属性情報を用いる参加型センシングの一つの例としてレストラン評価のための参加型センシングが挙げられる．そのようなセンシングでは，モバイル機器を有する参加者が，訪れたレストランに対する写真やコメントなどをサーバに送信し，共有する．また，参加者の属性情報をレストランの分類・位置付けのために利用する．例えば，ある店に良いコメントを書いた 20 代のユーザが多かったならば，その店を 20 代に薦める店として位置付ける．

このような参加型センシングで問題となるのは，参加者から送られる情報にプライバシーに関わる情報が含まれうることである．レストランを訪問する時間帯を分析することで，参加者がどのような生活をしているかが推測される可能性がある．また，評価の内容もセンシティブな情報であると考えられる．ここで単純にユーザの名前を秘匿するだけでは，プライバシーの保護は十分ではない．以下で述べるように，ユーザの属性情報を参照することにより，ユーザが識別されてしまう可能性があるためである．

我々のグループでは，[6] において位置に基づくサービス（location-based service, LBS）における属性を考慮したプライバシー保護手法を提案した．ユーザの属性（例：性別，年齢層）も活用する位置情報サービス（例：モバイル広告）において，サービスを要求したユーザが攻撃者（adversary）から観測されることを考慮し，近くに存在する属性が類似したユーザとグループ化して匿名化するものである．これを参加型センシングに拡張するには，その特徴を考慮した新たなプライバシー保護手法が求められる．

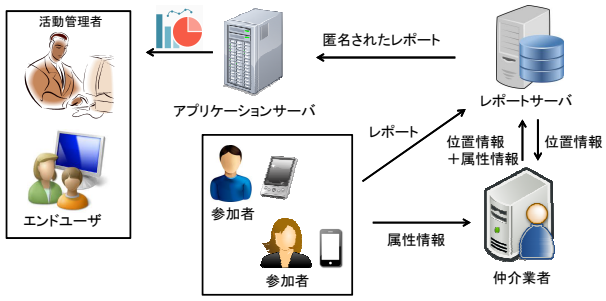

図 1: システムアーキテクチャ

本稿では，参加型センシングのための属性情報に着目したプライバシー保護手法について議論する．まず，システムアーキテクチャを説明し，発生しうる問題について述べる．その後，属性を考慮したプライバシー保護のためのアイデアについて述べる．

2 システムアーキテクチャ

本研究では，属性情報を用いる参加型センシングにおけるプライバシー問題に対して，図 1 のようなシステムアーキテクチャを想定する．

参加型センシングの参加者は，携帯機器を用いて**レポートサーバ**に情報を提供し，共有する．**アプリケーションサーバ**は集積されたレポートを分析し，参加型センシングの活動管理者やエンドユーザにアプリケーションを提供する．しかし，ここではアプリケーションサーバはネットワーク上のサービス等であり，必ずしも信頼できず攻撃者となる恐れがあると考える．そこで，**仲介業者**という信頼できるサードパーティを用いて，参加者の属性情報をプロファイルとして保存し，匿名化する．レポートサーバは参加者からのレポートから時空間データを抽出し仲介業者に送る一方，匿名されたレポートをアプリケーションサーバに送信する．

このようなアーキテクチャに基づき参加型センシングを行うが，プライバシーに関して以下のような問題が発生しうる．

1. データのスパース性（sparseness）：参加型セン

Privacy Protection Method for Participatory Sensing
Jing Zhao†, Tingting Dong†, Yoshiharu Ishikawa†§
† Graduate School of Information Science, Nagoya University
§ National Institute of Informatics

シングの参加者がある訪問先周辺にはあまり存在しない場合，人物が特定しやすくなる．レストランの例では，ある時点において対象のレストランを訪問した参加者がほとんどいなければ，他の情報と突き合わせて人物を推定することが容易になる．

2. トレース攻撃：同じ参加者による複数のレポートをリンクして分析すると，参加者を識別しやすくなる．例えば，図 2 では，各時点 t_1, t_2, t_3 おいて得られたレポートについて，各ユーザの属性値を匿名化している．具体的には属性「年齢」の値について汎化を行っている．これを見ると，ユーザ U_1 の年齢値範囲が異なる時刻では違う範囲に匿名化されている．そのため，攻撃者は t_1 と t_2 の年齢値を比べて，U_1 が 20 歳であると推定できる．

そこで，参加型センシングにおける属性情報も考慮したプライバシー保護の技術の開発が求められる．

時間	UID	年齢
t_1	U_1	[16-20]
t_1	U_2	[16-20]
t_1	U_3	[16-20]

時間	UID	年齢
t_2	U_1	[20-26]
t_2	U_3	[20-26]
t_2	U_4	[20-26]

時間	UID	年齢
t_3	U_1	[18-22]
t_3	U_5	[18-22]
t_3	U_6	[18-22]

図 2: 匿名化されたプロファイル

3 提案手法のアイデア

本研究では，属性情報を用いる参加型センシングにおいて，***k*匿名化** [7] の考え方にに基づくプライバシー保護を行う．すなわち，k 人の参加者が位置と属性の情報のもとで互いに区別されないようにする．このために，次の 2 つの考え方に基づいて匿名化を行う．

- **混同時間**：各訪問先に対して，匿名化のためレポートを送信した参加者をグループ化する必要がある．しかし，ある時点で同じ訪問先に訪問するユーザ数が少ない場合，データのスパース性により k 匿名化を実現することが困難になる．本研究では，状況に応じてある一定の長さの時間を設定し，その時間内の訪問イベントに関する匿名化を行う．この時間帯を**混同時間**（confusion time）と呼ぶ．その大きさは，その時間帯における対象訪問先周辺の参加者の人数に応じて決定する．
- **属性値の microaggregation**:属性情報に対しては，統計データベースでよく使われる *microaggregation* の考え方 [3] に基づき，k 匿名化を実現する．

匿名化処理では，上記の考え方をもとに 2 つ観点でのグループ化を行う．

1. 時間に基づくグループ化：参加者数が k 匿名化の指標を満たすように，時間帯の長さを徐々に長くしながら参加者をグループ化する．すなわち，混同時間は匿名化対象のデータに応じて動的に決定する．
2. 同値類の生成：ある時間帯に個々の訪問先に訪問した参加者に対して，類似する属性値（例：年齢）を持つ参加者をグループ化する．属性値の類似度は対象ドメインごとに与えられるものとする．

これら 2 つの観点に基づくグループ化を交互に進め，比較的短い時間帯の中で妥当な匿名化を得ることを目指す．

4 まとめ

本論文では，参加型センシングにおける参加者のプライバシー問題について，これまでの位置情報のみを考慮する匿名化手法に対し，属性情報も考慮する手法を提案した．今後は，手法のより具体的な詳細化と実証実験などに取り組みたいと考えている．

謝辞

本研究の経費の一部は科学研究費（25280039）および NEDO IT 融合プロジェクトによる．

参考文献

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In *First Workshop on World-Sensor-Web (WSW'06) (ACM Sensys Workshop)*, pages 117–134, 2006.

[2] A. Kapadia C. Cornelius and N. Triandopoulos. Anonysense: Privacy-aware people-centric sensing. In *ACM MobiSys*, pages 211–224, 2008.

[3] Josep Domingo-Ferrer and Josep M.Mateo-Sanz. practical data-oriented microaggregation for statistical disclosure control. *IEEE TKDE*, 14(1):189–201, 2002.

[4] K. L. Huang, S. Kanhere, and W. Hu. Towards privacy-sensitive participatory sensing. In *IEEE Percom*, pages 1–6, 2009.

[5] L. Kazemi and C. Shahabi. TAPAS: Trustworthy privacy-aware participatory sensing. *Knowledge and Information Systems*, 37(1):105–128, 2013.

[6] M. Mano and Y. Ishikawa. Anonymizing user location and profile information for privacy-aware mobile services. In *2nd ACM SIGSPATIAL Intl. Workshop on Location Based Social Networks (LBSN'10)*, pages 68–75, 2010.

[7] L. Sweeney. K-anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5):557–570, 2002.