位置情報プライバシ制御における匿名化マッチング方式

The method of anonymize matching in location privacy control

上茶 雄　　平野 美貴　　黒川 章
Jocha Tsuyoshi　Hirano Miki　Kurokawa Akira

NTT ネットワークサービスシステム研究所
NTT Network Service Systems Laboratories

1. まえがき

カーナビ、携帯 GPS 等の普及により、様々な位置情報サービスが増えている。現状のサービスでは位置情報の用途は限定されているが、今後のユビキタス社会では多様なコンテクスト、多様なサービスでの利用が増大すると期待される(図 1)。一方、ネット社会の普及により、プライバシ侵害等が社会問題化しており、プライバシ保護が広く望まれている。このような状況下、様々なコンテクスト・サービスに柔軟に対応可能な位置情報プライバシ制御方式の確立が課題となる。本稿ではその課題を解決するためのプライバシ制御方式における匿名化マッチング方式と許容誤差条件検査の検討について述べる。

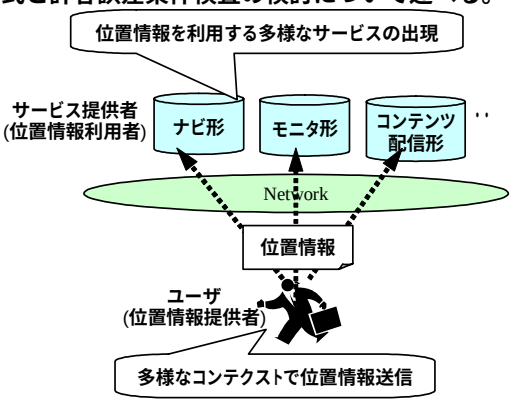

図1 ユビキタス社会における位置情報サービス

2. 要求条件と既存技術の問題点

2.1. 位置情報プライバシ問題とプライバシ制御技術

位置情報のプライバシ問題としては、二つが考えられる。一つは不用意に ID と位置情報を渡すことで、個人がどこに立ち寄ったかが知られてしまうという問題であり、もう一つは渡した位置情報からある場所にいた人物が特定されてしまう可能性があるという問題である。このような問題を解決する技術として、ポリシ制御技術と匿名化技術の 2 つがある。ポリシ制御技術は不用意な情報流出を防ぐために個人情報の流通をポリシ制御する技術であり、匿名化技術は渡した位置情報等を通じて相手に自分が特定されることを防ぐために位置情報の形式や抽象化度(解像度、精度)を変更する技術である。

2.2. 要求条件

要求条件として以下を考える。

- 多種・多様なコンテクスト(場所、時刻)で位置情報を送信する⇒コンテクストに応じて、位置情報をどのように送信するかをポリシ制御できること
- 多様な位置情報サービスの利用を妨げてはならない⇒位置情報はユーザのプライバシを保護しつつ、サービス提供側でも利用できる様に変換(匿名化)できること

2.3. 既存技術の問題点

2.3.1 ポリシ制御技術

ポリシ制御に関しては、W3C で議論されており、P3P[1] 、APPEL[2]等で仕様化、working draft 化されている。しかし、これらの対象アプリケーションは Web アクセスであるため、以下の問題点がある。

問題点 1：ポリシで記述できるのは情報収集者、収集項目、収集目的等のみであり、コンテクストに応じて出力条件を変更できない

問題点 2：比較後の動作は、接続許可・拒否等のみ記述可能であり、位置情報の匿名化条件を指定できない。

2.3.2 匿名化技術

匿名化技術に関しては、IETF geopriv[3]等で触れられているものの、具体的な方法の議論はされていない。階層化された情報をより上位のものにしていく手法(部屋名→フロア名→ビル名等)や解像度を粗くしていく手法(精度 10m→100m→1000m 等)が個別に提案されているのみである[4]。これにより、現状、以下の問題が生じる。

問題点 3：単純な抽象化のみでは、位置情報サービス提供者は様々な形式に変換した位置情報を利用するため、サービス利用の利便性が阻害される。

例えば、車両のナビゲーションでは、最寄の道路名・交差点情報、地域コンテンツ配信サービスでは、地名情報を利用すると考えられる。この場合、緯度・経度の有効数字を減らす等の単一の技術で抽象化度を大きくすると、誤差が大きすぎて利用できないことが考えられる。

3. 提案方式

3.1.前提とするアーキテクチャ

アーキテクチャに関しては P3P では仕様に特に記述はないが、基本的にはクライアントとサーバの 2 者間で動作するアーキテクチャとなっている。対して、geopriv では位置情報送信者と位置情報受信者の間の第三者がルールに応じて位置情報を提供するアーキテクチャとなっている。本稿では、「サービス提供者へ伝わるユーザの情報は極力減らす」、「低リソースな PDA 等をユーザ端末として許容する」という条件を考慮し、後者のユーザとサービス提供者の間に第三者(調停者)が入るアーキテクチャを前提とし、調停者が行うポリシ制御、匿名化機能の検討を行う(図 2)。

3.2. 調停者の機能条件

2.3.の問題点 1〜3 に対応した以下の機能条件を考える。

機能条件 1：ポリシ比較項目として、P3P で想定されているポリシ項目(情報利用用途、情報利用者、情報収集項目等)に加えて、ユーザのコンテクスト条件(位置情報、時刻)を追加する必要がある。

機能条件 2：ユーザの位置情報匿名化条件とサービス提供者の位置情報匿名化許容条件を比較し、位置情報の形式条件・抽象化条件(匿名化条件)を決定する必要がある。

機能条件 3：位置情報をサービス利用に適した様々な形

式に実際に変換し、さらに抽象化する必要がある。また、形式変換・抽象化(匿名化)後の位置情報がサービス提供者側の利用に問題がないかを検査する機構も必要となる。

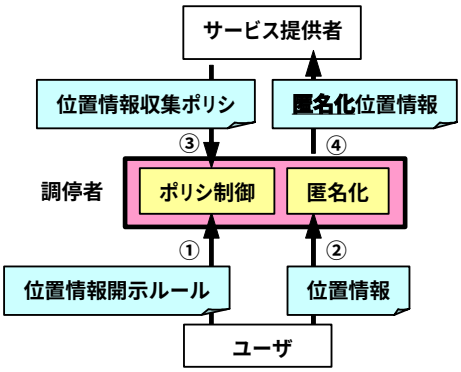

図2　プライバシ制御アーキテクチャ

3.3. 検討課題

3.3.1. 課題概要

上記の機能条件 1.～3.により、以下の課題が考えられる。

課題 1.コンテクスト条件追加によるユーザ設定稼動増

課題 2.位置情報形式変換・抽象化条件の比較方式

課題 3-1.位置情報形式変換・抽象化方法

課題 3-2. 形式変換・抽象化した位置情報の誤差検査方式

課題 1.に関してはコンテクスト分類による対応手法を提案している[5]。また、課題 3-1.については、地図情報データベースを利用することで、緯度・経度を様々な位置情報形式(地名形式、道路・交差点形式、駅名形式等)へ変換・抽象化が可能と考えられる。本稿では課題 2.、3-2.について詳細に述べる。

3.3.2. 課題 2. 位置情報匿名化条件の比較方式の検討

【課題抽出】ユーザのプライバシを守るためには位置情報の形式、抽象化度をユーザが指定する必要がある。また、サービス提供者の柔軟な位置情報利用を実現するためにはサービス提供者自身も位置情報形式や、許容可能な抽象化度を宣言する必要がある。よって、この両者の条件を満足するような匿名化条件を決定する必要がある。

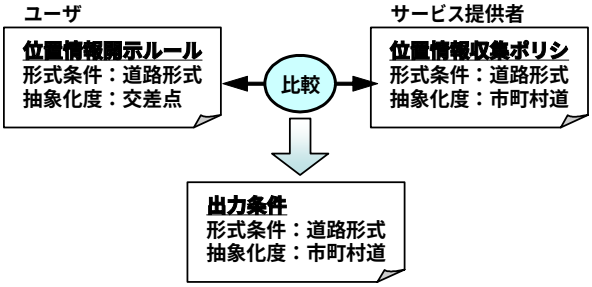

図3　匿名化条件マッチング例

【提案方式】図 3 を元に提案方式を説明する。位置情報形式条件に関しては、ユーザのルールとサービス提供者のポリシを比較し、同一の位置情報形式が含まれていれば、マッチング成功であり、出力条件はその位置情報形式とする(この例では道路形式)。これは、ユーザの位置情報開示ルールと位置情報収集ポリシの積集合をとることで実現可能である。

抽象化条件に関しては、位置情報収集ポリシの抽象化度がユーザの位置情報開示ルールの抽象化度より粗い場合にマッチング成功となり、出力条件はサービス提供者側の抽象化度とする。例では位置情報の開示ルールの抽象化度(交差点レベル)より位置情報収集ポリシの抽象化度(市町村道レベル)の方が粗いため、マッチング成功となり、出力条件は位置情報収集ポリシの抽象化度(市町村道レベル)となる。

以上により、ユーザ、サービス提供者双方の条件を満足することが可能となる。

3.3.3. 課題 3-2. 匿名化後の位置情報の誤差検査方式

【課題抽出】位置情報形式が緯度・経度や地名形式の場合、元の位置情報を内部に含んだ形で抽象化を行うので、誤差=抽象化度と考えることができる。しかし、道路形式や路線形式の場合の抽象化度は位置情報の示すエリアの範囲を表すため、ユーザの匿名化に対応する条件ではあるが、形式変換・抽象化後の道路名、駅名が真の位置に対してどの程度誤差がある(離れている)かが分からないため、サービス提供者側の位置情報収集条件としては不十分である(図 4)。よって、位置情報形式が道路形式や路線形式の場合、変換・抽象化後の道路等とどの程度まで離れていることを許容するかという許容誤差条件をポリシに追加し、実際に許容誤差内に収まっているかどうかを検査する機構が必要となる。

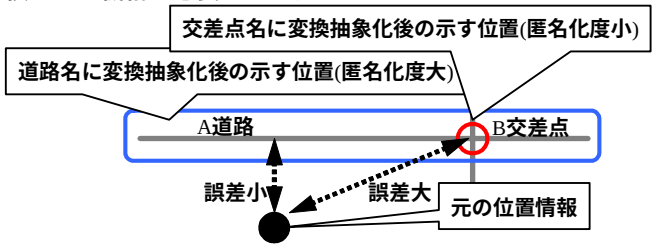

図4　抽象化度と誤差(道路形式の例)

【提案方式】変換・抽象化後の道路等と元の位置情報の距離を計算し、許容誤差と比較する方式、及び、最寄りの道路・交差点名に変換する際に変換対象の道路・交差点の検索範囲を予め、許容誤差以内の範囲のエリアに絞るという方式が考えられる。変換の効率性や変換時間を考慮し、後者の方式を提案する。これにより、位置情報を道路形式、路線形式等に匿名化する場合でもサービス提供者側の収集条件を満足することが可能となる。

4. まとめ

様々なコンテクスト・サービスに柔軟に対応した位置情報プライバシ制御を実現するプライバシ制御アーキテクチャを提案し、匿名化マッチング方式と許容誤差条件検査方式について検討した。今後は詳細検討、システムへの実装を進め、マッチング方式、匿名化方式のフィージビリティ評価、性能評価を行う。

5. 参考文献

[1]”The Platform for Privacy Preferences 1.0 (P3P1.0) Specification” W3C Recommendation,16 April 2002

[2]”A P3P Preference Exchange Language 1.0 (APPEL1.0)” W3C Working Draft,15 April 2002

[3]”draft-ietf-geopriv-reqs-04.txt” Internet Draft,Oct 2003

[4] M. Gruteser, and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” Proc. 1st International Conference on Mobile Systems, Applications, and Services, San Francisco, U.S.A., May 2003.

[5] 上茶雄,平野美貴,黒川章,”位置情報サービスにおけるプライバシ制御方式に関する検討”信学会ソサイエティ大会, B-7-73,2003