M-103

位置情報の自己改ざん防止のためのアドホックな検知機構の設計

Design of an Ad-hoc Detecting System against the Self Falsification of Location Based Services

佐々木 直志 † **安田 絹子** † **多田 好克** †‡
Tadashi Sasaki Kinuko Yasuda Yoshikatsu Tada

1. はじめに

信頼関係のないモバイルユーザ間で信頼性のある位置情報を送受信する場合、送信者自身が改ざんした位置情報を送ること **(自己改ざん)** への対策が必要である。たとえば、屋外ユーザに対応した配達サービスでは、悪意を持つユーザが現在位置を改ざんして事業者のサービス妨害・混乱を企むことが考えられる。従来の自己改ざん対策 [1][2] では改ざんの防止が行われている。改ざん防止対策では、位置情報送信などの制御能力が送信者から失われることが多い。このため、送信者の制御外で位置情報が不正に取得・蓄積される危険があり、送信者のプライバシ保護に問題があった。これらの問題を踏まえて、送信者から位置情報の制御能力が失われない周辺ユーザを利用するアドホックな改ざん検知機構を設計した。

2. 従来の改ざん対策

2.1 中央機構による対策

ユーザの位置情報を中央機構で管理し、中央機構が位置情報の信頼性を保証する対策である。一般的には、中央機構がユーザの位置を測位することでユーザによる改ざんを防止することが多い。この場合、ユーザの同意がなくとも位置情報を取得・蓄積することが原理的には可能である。

2.2 ハードウエアによる対策

送信者の機器にハードウエア的に隠蔽された部分を設ける対策である。送信者の不正な操作を物理的に防止する。しかし、送信者が制御できない機器をネットワークに接続することになるため、第三者による不正な位置情報収集の可能性を否定できない。また、測位システムごとにハードウエアを設計・生産しなければならないので、汎用的な対策ではない。

2.3 過剰対策問題

上にあげたどちらの対策にも共通する問題点として、選択的な適用が行えない点が挙げられる。位置情報の改ざんが問題ない場合でも、防止対策を停止することができない。たとえば、現在位置から地図情報のみを提供するサービスでは、位置情報が自己改ざんされてもサービス側に問題はない。この場合、改ざん防止対策はプライバシ問題の危険要因でしかない。

†電気通信大学 大学院 情報システム学研究科,
Graduate School of Information System,University of Electro-Communication,Japan.
‡産業技術総合研究所サイバーアシスト研究センター,
Cyber Asist Research Center,AIST,Japan.

3. システム設計

3.1 設計方針

従来手法の問題点を踏まえて、中央機構や送信者が制御できないハードウエアを用いない改ざん対策機構を設計した。設計では、送信者が改ざんを行うことで問題が起こるケースにのみ、選択的に改ざん検知を適用可能である。

3.2 想定環境

電子測位機能と、周辺端末との近距離無線通信機能をもつ個人用携帯端末が普及した社会環境を想定した。現在の携帯電話端末の普及率に近いレベルで想定した端末が普及し、各ユーザがそのような携帯し利用している状況を考えた。このような社会環境において、任意のユーザの**周囲 (近距離通信で通信可能なエリア内)** には、他のユーザが存在している可能性は高い。現時点では、近距離無線通信には IEEE 802.11b や Bluetooth、電子測位には GPS や位置同定センサを用いることで想定端末の機能を実現できる。

3.3 改ざん検知

本システムは、送信者周囲のユーザ **(ネイバー)** のグループ **(ネイバー集合)** と近距離無線通信を利用して、送信者の自己改ざんの有無を検知する。ネイバー集合は、送信者と近距離無線通信で通信可能であるユーザの集合であり、検知を行うたびに動的に構成される (図 1)。また、送信者の周囲に偶然位置していたユーザの集合なので、送信者と受信者の両方に利害関係を持たない。送信者 (被検証者) と送信者の周囲の複数のユーザ (ネイバー集合) が近距離無線通信可能であるかを調べた結果と、各ネイバーの現在位置を受信者 (検証要求者) に通知する。受信者 (検証要求者) は、通知された結果を基にして位置情報が改ざんがされていた確率を求めて、改ざんの検知を行う。

3.4 ネイバー集合の性質

ネイバー集合に含まれるネイバーは、送信者から一定距離内に偶然に位置していた第三者であり、送信者と受信者に対して利害関係はないと考える。ネイバー集合は複数の異なるネイバーから構成されるので、悪意を持って検知に参加するネイバーがいることも考えられる。しかし、大多数のネイバーは利害関係がないため、検知結果を故意に歪める必然性がない。また、複数のネイバーと送信者との近距離通信の結果から改ざん確率を求めるため、悪意を持つ少数のネイバーだけでは、結果である改ざん確率を大きく変更することは難しい。

3.5 検知対象の位置情報

本検知機構で対象とした位置情報は、現在時刻 T に近い時間 $T \pm \Delta$ での位置 (現在位置) である。許容される

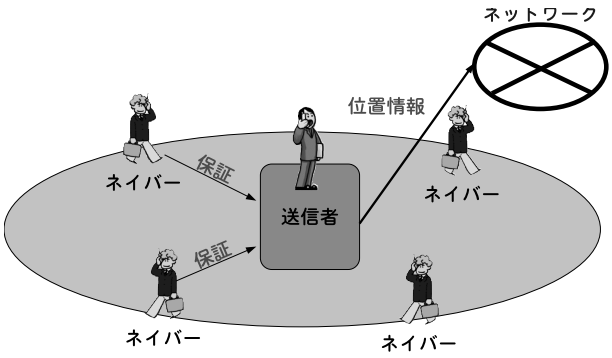

図 1: ネイバーとの関係

時間 Δ は周辺ユーザによるグループの状態が大きく変化しない時間である。本研究では、送信者と周辺ユーザの平均的な移動速度から事前に決定しておくものとした。

3.6 ネイバー参加の判断

送信者からネイバーとして保証に参加するよう要請があったユーザは、検知に協力するかを判断することができる。この際、常に手動で判断するのではなく、事前に設定されたポリシーに従って検知依頼に対して応答することを考えている。

ポリシー例

- 移動速度:送信者との相対的な移動速度が速い場合は参加しない
- 負荷率:端末の負荷率が高いなら参加しない
- 参加回数:一定時間内に規定回数しか検知に参加しない

4. 検知フロー

この検知フローで求めている情報は、送信者のネイバー集合 N の部分集合 N' に含まれるユーザ $\forall a \in N'$ から見たネイバー集合 N_a と、集合 N との積集合 $N \cap N_a$ である。受信者は $N \cap N_a$ の集合の大きさから改ざんされている確率を求める。

1. 検知実行要求：受信者⇔送信者
2. ネイバー集合 N の探索:送信者⇔ネイバー
   - 送信者:ネイバー集合の作成要求を現在位置や状態を含めてブロードキャストする
   - ネイバー:参加ポリシーから検知に参加するかを判断
   - ネイバー:検知に参加する場合は参加応答を返す
3. 改ざん検知:受信者⇔ネイバーの一部 (図 2)
   - 受信者:ネイバー集合 N に含まれる集合 $N' \subseteq N$ を設定
   - ネイバー $\forall a$：ユーザ a から見たネイバー集団 N_a を作成
   - ネイバー $\forall a$:集合 N と N_a の積集合 $N \cap N_a$ とネイバー $\forall a$ の現在位置を受信者に通知
4. 改ざん確率の導出：受信者
   - 受信者：積集合から改ざんされた確率を求める

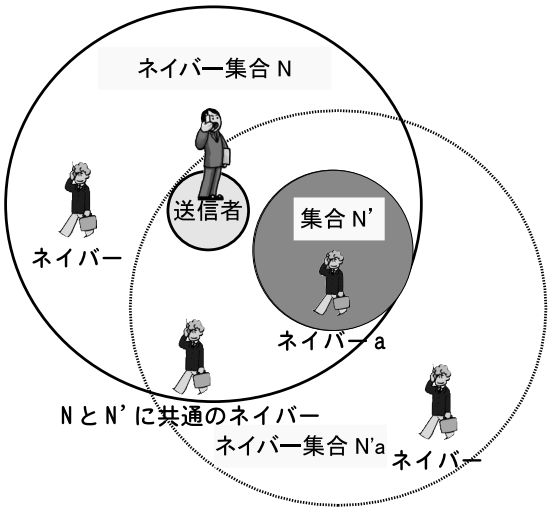

図 2: ネイバー集合を用いた改ざん検知

5. 現状

実験端末として、近距離無線通信に IEEE 802.11b、電子測位に GPS を選択し、実験を行う予定である。

6. まとめと今後の課題

本稿では、送信者自身が現在位置を改ざんして送信する問題 (自己改ざん) の対策として、将来的に実現可能なモバイル機器のユーザを用いる改ざん検知機構を提案した。従来の改ざん対策では、送信者の位置情報の制御能力が損なわれ、送信者側の位置情報を第三者が不正に得られる危険性があった。本機構では、送信者の制御能力を損なわずに、改ざんを検知可能な情報を受信者が得ることができる。しかし、送信者に協力して現在位置を提供する**検知代行者**が送信者になりかわって不正な検知結果を受信者に与える問題や、各端末の時計誤差や測位誤差の検知への影響など解決すべき問題も多い。今後の課題は、改ざん対策の一つとして、本機構の有効性を実験から明らかにすることである。

参考文献

[1] Debbie Caswell and Philippe Debaty,“Creating web presentations for places,” Proceedings Handheld and Ubiquitous Computing 2000, pp.114-126, Springer, 2000.

[2] Peter F. MacDoran, Michael B. Mathew and et al, “METHOD AND APPARATUS FOR AUTHENTICATING THE LOCATION OF REMOTE USERS OF NETWORKED COMPUTING SYSTEMS,” US. Patent Number 5757916, May 26 1998.