平成15年度 修士論文

近隣端末間の相互保証による
位置情報改ざん検知機構の設計と評価

電気通信大学 大学院情報システム学研究科

情報システム設計学専攻

0250018 佐々木 直志

指導教官 多田 好克 助教授
星 守 教授
橋山 智訓 助教授

提出日 平成16年1月30日

目 次

第 1 章　序論 **7**

1.1 背景 7

1.2 研究目的 9

第 2 章　関連研究 **10**

2.1 位置情報提供システム 10

2.1.1 携帯電話網 10

2.1.2 PHS 11

2.1.3 Enhanced-911 12

2.1.4 Cyber Locator 12

2.1.5 GLI システム 13

第 3 章　自己改ざん対策の比較 **14**

3.1 ハードウエアによる対策法 14

3.2 外部観測による対策 15

第 4 章　システム設計 **17**

4.1 本研究の保証方法 17

4.1.1 問題点 18

4.2 想定する環境と前提条件 19

4.2.1 想定端末 20

4.2.2 ユーザと端末 ID の対応 20

4.2.3 第三者の存在 21

4.2.4 歩行者密度 21

4.2.5 前提条件のまとめ 22

4.3 システム構成要素 23
4.4 検証手順の詳細 23
4.5 必要な保証者数 24
4.5.1 検証者の選択人数 25
4.6 検証によって得られる情報 26
4.7 指標値の計算方法 26
4.8 シナリオ 29
4.9 結託者対策 35
4.9.1 結託者の最大数 35
4.9.2 結託者の枯渇 35
4.9.3 周囲の第三者数 36
4.9.4 結託者の戦略 37

第 5 章 シミュレーション 38

5.1 実験環境 38
5.1.1 実験空間 38
5.1.2 物理パラメータ 39
5.1.3 通信手順 39
5.2 基礎実験 41
5.2.1 歩行者密度と保証者数 43
5.3 改ざん検知実験 45
5.3.1 実験 1:結託者の集中使用 45
5.3.2 実験 2:結託者の確率的使用 48

第 6 章 問題点と課題 51

6.1 端末 ID 収集の問題 51
6.2 過去データとの比較による改良 52

6.2.1 ID 一致数 52
6.3 指標値の計算方法 53
6.3.1 保証者を利用した指標値 53
6.3.2 検証者の位置を使った指標値 55

第 7 章 おわりに 57

図 目 次

1.1 緊急通報と自己改ざん 7

3.1 ハードウエアによる対策 15
3.2 外部測位による対策 16

4.1 本システムの保証方法 19
4.2 位置保証が必要ない場合 19
4.3 再帰的な検証 24
4.4 要求者が得られる情報 (D=3 の例) 26
4.5 修正後ツリー (D=3) 28
4.6 指標値の計算例 (D=3) 29
4.7 保証者要求 (通常) 29
4.8 保証者要求 (自己改ざん) 30
4.9 保証者応答 (通常) 31
4.10 保証者応答 (自己改ざん) 31
4.11 検証実行 (通常) 32
4.12 検証実行 (自己改ざん) 33
4.13 保証手順繰り返し (通常) 33
4.14 保証手順繰り返し (自己改ざん) 34

5.1 通信シーケンス 42
5.2 保証者数 (密度 2000 人/平方 km^2, 検証者数 ≤ 6) 47
5.3 保証者数の累積比 (密度 2000 人/平方 km^2, 検証者数 ≤ 6) 47
5.4 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 20%結託者) . . . 48
5.5 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 50%結託者) . . . 49

5.6 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 70%結託者) . . . 49
5.7 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 90%結託者) . . . 50
5.8 指標値比較 50

6.1 位置によるグループ化 54

表 目 次

4.1 シミュレーションに用いたデバイス 20
4.2 構成要素分類 23

5.1 通信トークン 41
5.2 ユーザ数と保証者数 44
5.3 基礎実験での統計データ (歩行者密度 2000 人/平方 km^2) 46

第 1 章

序論

1.1 背景

近年、移動体通信などのネットワークを利用した個人向けの位置情報システムが実用化されつつある。例えば、GPS 付き携帯電話を端末に用いた歩行者の経路誘導 (歩行者ナビゲーション) システムなどである。歩行者ナビゲーションでは、利用者の位置情報をネットワークでサービス提供者に送り、サービス提供者は、利用者が送信する位置情報をもとにサービスを行う。これらの位置情報サービスの中には、利用者の位置情報が利用者と正確に対応していることの保証 (位置保証) が必要なものがある。

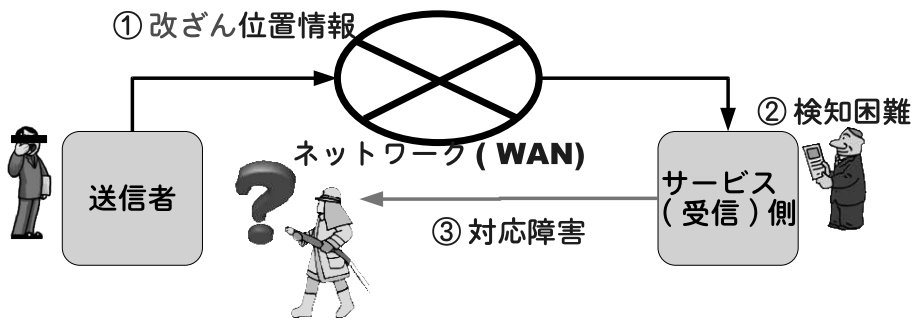

図 1.1: 緊急通報と自己改ざん

たとえば、位置保証が必要なサービスとして、屋外の利用者の指定場所に荷物を配達する位置情報サービスが挙げられる。このようなサービスのために、ネット

ワークを経由した位置情報の保証方法や保証システムが存在する [1]。しかし、これら既存の保証システムには、利用者自身が故意に位置情報を改ざんできる自己改ざん問題があり、それによるサービス妨害が可能である。

一例として、消防や警察へ携帯電話で緊急通報する場合を考える。携帯電話で緊急通報すると、口頭で通報位置を伝えるように求められる。このとき通報者が通報位置を誤って伝えると緊急車両が目的地に到着できず、対応が遅れることが問題となっている。また、警察や消防を混乱させる悪意を持った通報者が、自己改ざんによって嘘の通報位置を伝えても、携帯電話からの情報のみでは位置を確認することができない。実際に通報現場にいって確認しなければならず、悪意を持つ者が目的を達成してしまう。位置保証の自己改ざん防止はこのような場合に必要である。

現在、位置保証システムはハードウエアによる対策が主流であるが、対策コストが大きいという問題がある。これは物理的保護された特殊な端末が必要であることが主な原因である。

緊急通報の実例では、アメリカ政府が携帯電話での緊急通報のための位置保証対策 (Enhanced 911[2]) を推進している。しかし、全米の携帯電話全てを特殊端末に交換する必要があり、コストの面で計画の実施は遅れている。

近年、携帯電話や無線 LAN などのモバイル通信の方式が多様化し、位置同定技術も、GPS、センサ、電子ジャイロなど種類が増えている。これらの機器は年々安価になっているが、現在の位置保証技術はその対策に特殊端末を必要とするため、価格低下の恩恵を受けることができない。特殊機器の利用は、位置保証システム構築コスト削減の阻害要因になっている。

1.2 研究目的

本研究の目的は、利用者自らが現在位置情報を改ざんしてネットワークに送信し、遠隔地のサービス者を欺く自己改ざんへの対策方法を、汎用的な端末機器のみを用いて行うことである。本研究では、GPS や無線 LAN などの安価で汎用的な機器のみを用いる。つまり、特殊構造を持つ専用端末でのハードウエアによる保護ではなく、統計的なアプローチで自己改ざん対策を行う。本研究のような手法をとることで、近年出現した新しい安価な機器を用いた位置同定技術においても自己改ざんの対策が可能となり、位置保証システム構築コストの削減も可能となる。

第 2 章

関連研究

2.1 位置情報提供システム

本章では、位置情報を提供する各種システムを、その仕組みを中心にして概観する。

2.1.1 携帯電話網

携帯電話端末は、携帯電話専用に設計された特殊設計機器であるが、販売数が多いなどの理由から端末価格は安価である。現在主流のセルラ方式の携帯電話では、端末と通信可能な基地局との対応を常に把握する階層的な位置登録機構が存在する。基地局の位置は既知であるので、基地局と通信可能な携帯電話端末は、基地局の電波が到達する地理エリア (セル) 内にいることがわかる。

携帯電話での自己改ざん問題とは、同一の端末識別 ID を複数の端末に設定することである。重複した ID を持つ端末を、一般にクローン端末と呼ぶ。クローン端末の通話料金は、正規の端末利用者に転嫁されてしまい正規利用者に被害が生じる。事業者にとっても、請求金額の信頼性が失われるため大きな問題である。

しかし、クローン端末は現実には問題となっていない。これは、携帯電話事業者は通話を成立させるために、端末を含むセルを常に把握しているためである。異なるセルに同じ ID の端末が同時に存在すると、事業者はクローン端末の存在を把握できるので、クローン対策を講じることができる。これは位置情報の自己改ざ

ん検知機構に他ならない。このため、クローン端末が存在したとしても端末とセルの対応関係は保証される。このように、携帯電話網は自己改ざん対策機構を持つ位置情報の保証システムの一つである。

一方、セルラ方式のセルの半径は数 km オーダなので位置精度は高くない。次世代の CDMA 方式携帯電話では、セルラ方式よりも位置精度は高いが、どちらも、位置情報を事業者以外が利用するのは難しい。セルと端末の対応把握は、事業者が通話を成立させるための内部情報であり、基本的に外部への提供はしない。

2.1.2 PHS

PHS は携帯電話網とシステム構成は同じであるが、セルラ方式携帯電話よりもセル半径が小さいため、より高い精度で保証された位置情報を得られる。国内では、NTT ドコモ社の「いまどこサービス」が利用できる。このサービスを契約すると PHS 端末の現在位置をその端末を含むセルの位置から求めて、電話や FAX で提供してくれる。このサービスは実際に子供の迷子防止や徘徊老人の保護などに使われている。セルが小さい以外は、携帯電話とシステムの基本構造は同一であり、「いまどこサービス」は自己改ざん対策機構を持つと言える。

しかし、端末を持つ人間の位置を外部から把握できるため、プライバシ保護の必要がある。いまどこサービスでは、問い合わせをできるのは、事前に登録した端末契約者の近親者に限定されている。緊急事態であっても、第三者が問い合わせをすることはできない。また、日本国内では音声、データ通信目的の利用者が携帯電話に移行しており、PHS 自体の利用者数が減少している。

2.1.3 Enhanced-911

Enhanced 911[2] は米国 FCC(連邦通信委員会) が定めた、携帯電話からの緊急通報に関する勧告である。勧告では、携帯電話からの緊急通報時に、通報位置を自動通知できるようにすることを求め、周囲状況による要求精度も定めている。

FCC は、米国内全ての携帯電話事業者が Enhanced 911 への対応を 2005 年までに終えるように求めている。現在、一般の固定電話では、緊急通報時に電話番号から通報場所が自動的に救急機関に通知されるようになっており、対応の迅速化に役立っている。しかし、従来の携帯電話には通報位置を自動通知するシステムが用意されていなかった。

Enhanced 911 勧告が要求する位置精度の条件を満たすには、携帯電話端末を GPS 付き携帯電話にするなどのシステム変更が必要であり、費用の問題で導入は遅れている。GPS 付き携帯電話は、GPS の測位データを機器内部で保護する。GPS 付き端末の自己改ざん対策は、特殊機器を用いた自己改ざん対策に分類される。なお、Enhanced 911 は米国の国内のみに向けた勧告であり、日本を含む他の国々には Enhanced 911 は適用されていない。

2.1.4 Cyber Locator

特殊な GPS 受信機を持つ送信者の測位を、ネットワーク経由で受信側がコントロールする Cyber Locator と呼ばれる特許 [1] が 1998 年に米国で成立している。Cyber Locator は特殊な GPS 受信機を使用し、ハードウエアと測位方式に深く依存した対策であり、汎用的な機器の利用はできない。

2.1.5 GLI システム

GLI (Geographic Location Information) システム [3] は、モバイル通信端末の位置情報を登録サーバで集中的に把握・管理し、端末の IP アドレスと位置情報とを相互に変換可能にするシステムである。

モバイル通信端末は、GPS などの測位機器で求めた現在位置情報 (経度, 緯度) を、ネットワーク経由で定期的に位置登録サーバへ登録する。位置登録サーバは、地理的な範囲を指定した検索を受付け、指定範囲にいるモバイル端末の IP アドレスリストを与える。利用者は、地理範囲と IP アドレスの対応関係を知ることができる。GLI システムには保証機構自体がなく、自己改ざん対策は行われていない。そのため、検索結果が実際のモバイル端末位置と正しく対応しているかを保証することはできない。

また、中央的なサーバ機構を用いているため、サービスのスケーラビリティに問題がある。全てのモバイル端末が定期的に位置情報をサーバに送信するため、端末数が増加すると定常的に高いネットワーク負荷が生じてしまう。この問題を解決するために、複数の位置登録サーバを階層構造にレイアウトして負荷分散を行う改良システム [4] も研究されている。

第 3 章

自己改ざん対策の比較

3.1 ハードウエアによる対策法

ハードウエアによる対策法は、測位機能を含む端末内部を非公開の方法で物理的に防護する方法である [1]。こうした方法では機器の改変を防ぐことで位置情報の送信者による改ざんを防止する。一般に、物理的な防護を行ったハードウエアを、耐タンパ性を持つハードウエアと呼ぶ。耐タンパ性を持ったハードウエアを用いた端末では、特定の受信者のみが復号できるように機器内部で位置情報を暗号化し、端末所有者の改ざんを防止する。また、ハードの改変を検知した場合には動作を停止するなどの対策が施されている。

ハードウエアによる保護対策の具体例として、現金輸送車の位置把握用システムの端末が挙げられる。輸送中の現金輸送車の現在位置は、常に監視センターが把握管理している。緊急事態に、端末の破壊や不正操作で位置情報を改ざんされないようにするためには、ハードウエア的な保護が確実である。

この方法の問題は、端末のコストが高いことである。原因は、内部構造を秘匿するために位置情報サービスごとに個別に開発する必要があるためである。

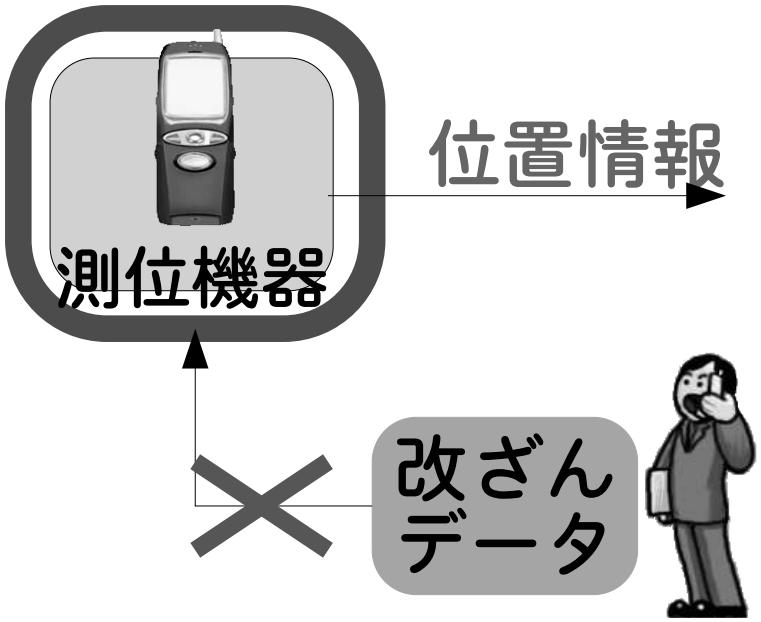

図 3.1: ハードウエアによる対策

3.2 外部観測による対策

外部測位は、事前に用意された観測システムで、外部から端末の位置情報を求める方法である。測位を端末所有者の外部から行うため、自己改ざんを行うことができない。この方式では自己改ざんは原理的に不可能である。

この方法を採用しているシステムに、Active Badge[5] や携帯電話網がある。Active Badge は超音波センサを使った室内向けのシステムである。屋外を含めたシステムには携帯電話網での携帯電話の位置把握がある。携帯電話網では各端末と通信できる基地局を常に把握しておく必要がある。

外部観測での問題点は、観測エリアが広い場合は多数の観測機器が必要で費用がかかることである。

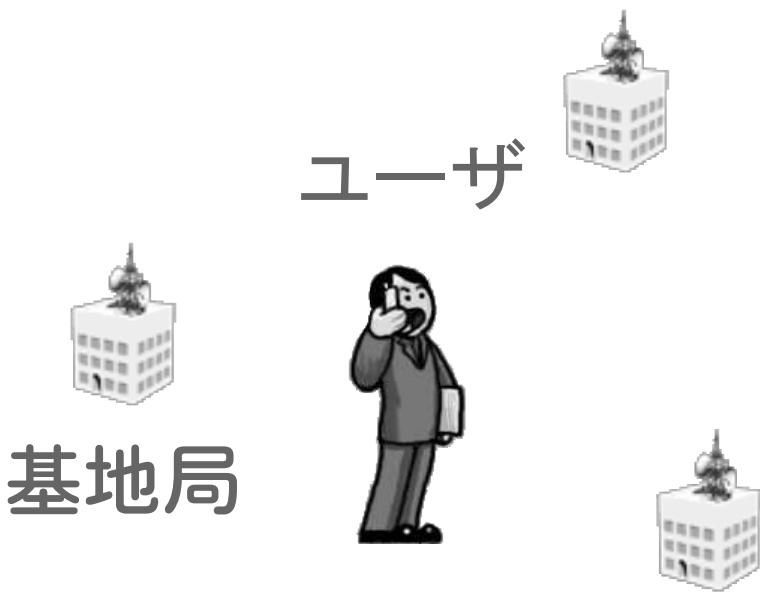

図 3.2: 外部測位による対策

第 4 章

システム設計

本研究システムは、汎用の端末を持った利用者について、その現在位置情報が自己改ざんされている可能性の指標値を求めるシステムである。この指標値により、自己改ざんが行われた可能性の検証を可能にする。本システムでは、周囲に同様の汎用端末を持った第三者が存在するなど、ある一定の条件が成り立つ場合に指標値を得ることができる。本システムは従来対策のように自己改ざんを根本から防止したり、周囲の状況に関係なく自己改ざんから位置情報を保護したりするものではない。本システムは従来対策を全て置き換えるものではなく、従来対策と相互補完的に利用可能な自己改ざん対策の新しい方法の一つである。

4.1 本研究の保証方法

本研究の位置保証は、ユーザの現在位置周辺にいる第三者ユーザによるユーザの存在確認をもとにして行う。本システムでは、近距離の通信ができる機器 (たとえば無線 LAN) と比較的安定した通信のできる機器 (たとえば携帯電話) ならびに電子測位機器 (たとえば GPS) の 3 つの機能を有する携帯端末を持っていると仮定する。なお、以下では無線 LAN、WAN 通信、GPS と略記する。

本システムによる位置保証の流れを図 4.1 で説明する。図中の利用者および周囲の第三者は本システムが仮定する端末を持っている。利用者は携帯電話 (WAN) を通じて電子測位 (GPS) で求めた位置を送信する。サービス側が位置保証を必要

としない場合は、利用者に対して周囲にいる第三者のリスト (端末の ID 番号など) の送信を求める。利用者は、無線 LAN で周囲の第三者と通信し、確認を依頼する。周囲の第三者は、確認結果をサービス者に送信する。最後にサービス者は、確認結果から利用者の位置が正しいことを確認する。

以上の説明では、GPS や携帯電話などの具体的なデバイスを使っているが、実際にはこれ以外のデバイスでも実現可能である。耐タンパ性の機器を仮定しないため、前述の 3 つの機能を持つ端末であれば、ユーザはサービスにあわせてデバイスを選択できる。また、サービス者が位置保証を必要としない場合は、図 4.2 のように保証手順を省いて、受信した位置情報を利用することもできる。

4.1.1 問題点

本システムには位置情報を送った利用者と確認を行う周囲の第三者が協力したときに、正しい結果がサービス者に得られない問題がある。この利用者と第三者の結託を本研究では結託者問題と呼ぶ。また、結託していない第三者の中にも、いいかげんな確認結果を送信する者がいる場合も考えられる。本研究ではこれを無確認問題と呼ぶ。本研究では、こうした結託者問題、無確認問題の対策も検討する必要がある。

1. 保証方法：(複数の) 周囲の第三者が利用者を確認し、存在確率を導出
2. 信頼性の基盤：周囲の第三者の集団の信頼性 = 位置情報の信頼性
3. 特徴
    - 保証が必要ない場合は保証手順を行わないことができる (図 4.2)
    - 機器非依存：保護された機器を必要としない
4. 問題点：

- 結託者問題：利用者と結託した第三者による不正
- 無確認問題：いいかげんな確認結果を送る第三者による誤認識

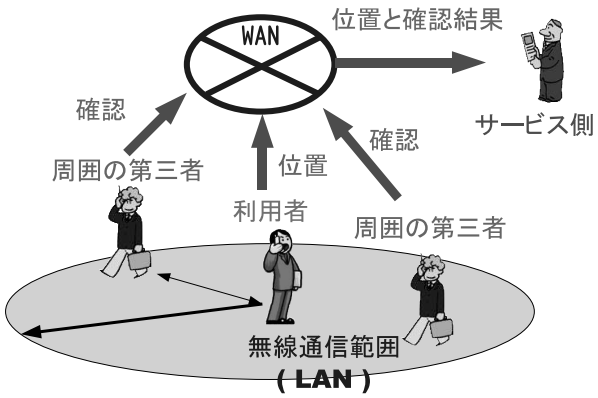

図 4.1: 本システムの保証方法

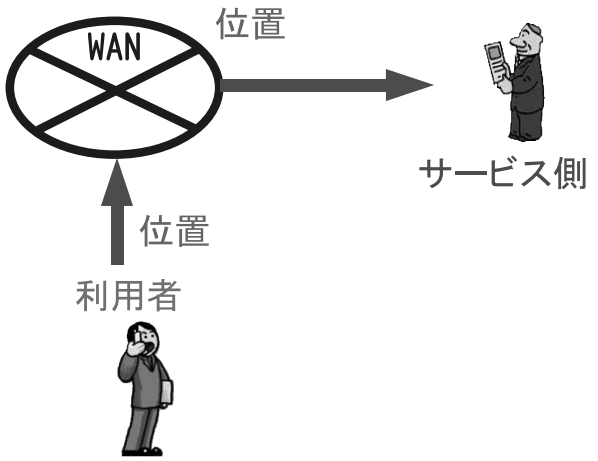

図 4.2: 位置保証が必要ない場合

4.2 想定する環境と前提条件

本節では、本研究が想定する実世界環境について述べる。本システムは、以下にあげる 4 つの条件がそろった状況で運用されることを想定している。

4.2.1 想定端末

本研究では 1) 近距離無線 と 2)WAN 通信 と 3) 電子測位 の 3 つの機能を持った個人用携帯端末が普及していると想定する。(これ以降、本研究で利用する携帯端末を、端末と表す)

想定する端末では、携帯電話と同様にユーザ全体で一意な ID が事前に設定済であって、かつ、端末には検証手順に応じて情報を提供する能力があるものとする。また、想定端末の計算能力・メモリ量は、現在市販されているプログラム実行可能な携帯電話と同程度のスペックであるとする。

2004 年現在、携帯電話では、無線 LAN (Bluetooth) 機能を持つ携帯電話、GPS 機能を持つ携帯電話などが市販され多数のユーザが利用している。3 つの機能をあわせ持った端末が近い将来に普及する可能性は高いと考えられる。

具体的な想定端末のスペックとして、表 4.1 のようなデバイスを想定し設計及びシミュレーションを行った。

表 4.1: シミュレーションに用いたデバイス

機能名	選択デバイス	目的
近距離無線	IEEE 802.11b (無線 LAN)	周囲の端末ユーザの探索と通信
WAN 通信	携帯電話 (パケット通信)	インターネット接続
電子測位	GPS	ユーザの現在位置を得る

4.2.2 ユーザと端末 ID の対応

本研究では、想定端末が現在の携帯電話端末と同様の取扱いができる端末であるとする。ほとんどの携帯電話ユーザは、端末を他人に預けることはしない。この

ため、携帯電話端末 (端末 ID、電話番号) とユーザ (人間) とは 1 対 1 の対応関係は成り立つと言って良い。

電子測位システムでは、GPS 受信機など対応する機器の現在位置を求めることはできるが、機器を持っている人間が誰であるかを示す情報は得られない。ユーザ間で端末の交換が可能であるなら、端末 (端末 ID) とユーザ (人間) とが 1 対 1 の対応関係であるとは言えない。

自由な交換の防止策として、正規所有者の指紋などを確認する生体認証が考えられる。しかし、生体認証に使用される機器は、特殊な専用機器であることが多い。本研究の目的の一つは、汎用的な機器のみで位置検証を実現することであり、生体認証機器の利用は本研究の方向性に合致しない。

ユーザが携帯電話端末を交換しない理由としては、自分宛にかかってくる電話を受けられないからであることが挙げられる。このとき、電話をかけた側では通話相手が本来の相手かどうかを、音声からある程度判別できる。また、電話帳や e-mail ログなどのパーソナルデータが端末に含まれていることも、理由の一つである。想定端末でも、同様に個人認証に使う認証鍵などのパーソナルデータが保存され、他人と交換することが困難であるものとする。

4.2.3 第三者の存在

本システムでは、利用者の周囲の第三者から送られる確認結果をもとにして、利用者の位置を検証する。このため、想定端末が社会に普及し、端末を携帯した多くのユーザのいる市街で利用されることを想定している。

4.2.4 歩行者密度

要求者は、位置情報をもとにして周囲エリアの統計的な歩行者密度を得ることが可能であるとする。歩行者密度とは、周囲を歩行している第三者の密度のことである。歩行者密度は一般に公開された情報でよく、秘密情報である必要はない。

本検証手順では要求者が歩行者密度を検知に利用する。送信者が送信した位置情報から、周囲の歩行者密度を求める。

都市部での歩行者密度の情報は、警察機関や携帯電話事業者などが所有している。現在は、一般には公開されていない。しかし、今後、位置情報サービスに必要な基本的な情報として一般公開向けに整備されていくと考えられる。

4.2.5 前提条件のまとめ

まとめると、本システムの前提条件は次の 4 つとなる。

1. 近距離無線、WAN 通信、電子測位の 3 つの機能を持つ想定端末の普及
2. 一意の端末 ID でユーザを識別可能で、ID とユーザは正しく対応すること
   - ID の不正変更：できないこと
   - 端末交換：他者と端末を交換することにデメリットがある端末 (携帯電話など)
3. 周囲に第三者が存在していること
4. 歩行者密度の統計情報の存在

4.3 システム構成要素

本システムでは、第三者に依存する自己改ざんの検証を行うため複数人がシステムの構成要素として参加することになる。表 4.2 に本システムを構成する各要素と、その説明を示す。

表 4.2: 構成要素分類

要素名	説明
移動者	位置情報 $Geo(x, y)$ の送信者
要求者	$Geo(x, y)$ の検証の要求者
保証者	移動者の存在を保証する第三者
検証者	移動者を直接確認するために、保証者の中から選ばれる
結託者	移動者と結託した保証者、検証者
近距離無線	周囲の端末間の通信に使用 (IEEE 802.11b)
WAN 通信	要求者との通信に使用 (携帯電話)

4.4 検証手順の詳細

本システムの検証の具体的な各手順を述べる。本システムは必要な人数の保証者 (ここでは N 人とする) を集めるために再帰的なアルゴリズムを使い、図 4.3 のように、移動者に近い第三者の存在を遠方の第三者が検証することを繰り返す。

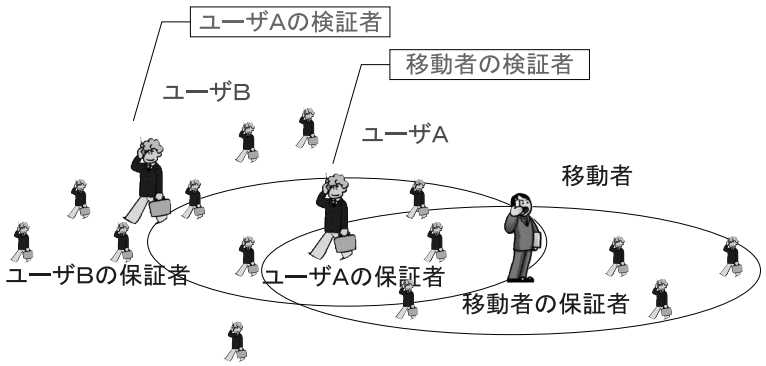

図 4.3: 再帰的な検証

4.5 必要な保証者数

要求者は、4.2.4 節の前提条件 (歩行者密度の統計情報) と移動者の送信した位置情報から、得られる保証者数の期待値を計算する。本研究では、シミュレーション結果 (5.2.1 章) から期待値の計算式を求めて利用した。要求者は期待値以上の保証者数を獲得できるまで検証を繰り返す。

検証手順

1. 要求者は移動者の現在位置を携帯電話で要求 $Geo(x, y)$ を受信する。
2. 要求者は移動者に携帯電話で位置確認のための保証者要求を送信する。
3. 移動者は周囲の第三者に無線 LAN で保証者となるよう依頼する。
4. 依頼された保証者は要求者に、移動者の保証者となったことを携帯電話で送信する。
5. 要求者は保証者の中から、移動者を確認する検証者を m 人[1]選び、携帯電話で確認を依頼する。ただし、すでに他の検証者の保証者となっている保証者

[1] m は要求者が設定できるが、以後本論文では 2 人と仮定して説明する

は除外する。

6. 検証者は移動者の存在を無線 LAN で確認し、確認結果を携帯電話で要求者に送信する。

7. 要求者は個々の検証者を新たな移動者と考え、以下の終了条件のいずれかが満たされるまで 1. ~ 6. の検証手順を再帰的に適用する。

   (a) 終了条件 1 : 新しい保証者が得られない

   (b) 終了条件 2 : 保証者数の合計が、要求者が設定した人数 N を越えた

本システムは、移動者の位置情報の信頼性を、移動者周囲の多数の第三者からの確認情報で求める。再帰的な検証の実行は、第三者の数を増やし、改ざん可能性の指標値の精度を高めるために行われる。

4.5.1 検証者の選択人数

本検証手順は、移動者を無線 LAN で確認する検証者を保証者の一部 (最大 2 人) を選んでいる。全ての保証者が検証を行わなくとも、自己改ざんを検知できる。

要求者は、多くの保証者を検証者に選択することも可能できるが、検証手順に必要な通信回数が増大し、以下に述べる二つの点で問題がある。

第一に、移動者の無線 LAN 機能に大きな負荷がかかるため正常な検証が行えなくなる問題がある。移動者の端末能力以上の多数の検証者が同時に検証を行うと、規定時間内に応答を得られなかった検証者は、誤った検証結果である「確認失敗」を要求者に送信してしまう。

第二の問題として、無線 LAN で同時に多数が通信を行うため、検証に無関係な周囲ユーザの通信にも影響を及ぼす。多数の検証者が同時に無線 LAN で通信すると、近隣の無線帯域が減少するため影響が大きい。

以上の 2 つの問題点から、保証者から多数の検証者を選択することは現実的でない。

4.6 検証によって得られる情報

検証手順の終了後、要求者には図 4.4 のようなツリー状の情報が得られる。以下、本論分ではこれを検証者ツリー と呼ぶ。移動者 (根) から見た各検証者 (節) までの距離が i の検証者を、i 次検証者と呼ぶ。また、要求者から最も遠い検証者までの距離 (ツリーの深さ) を D とする。

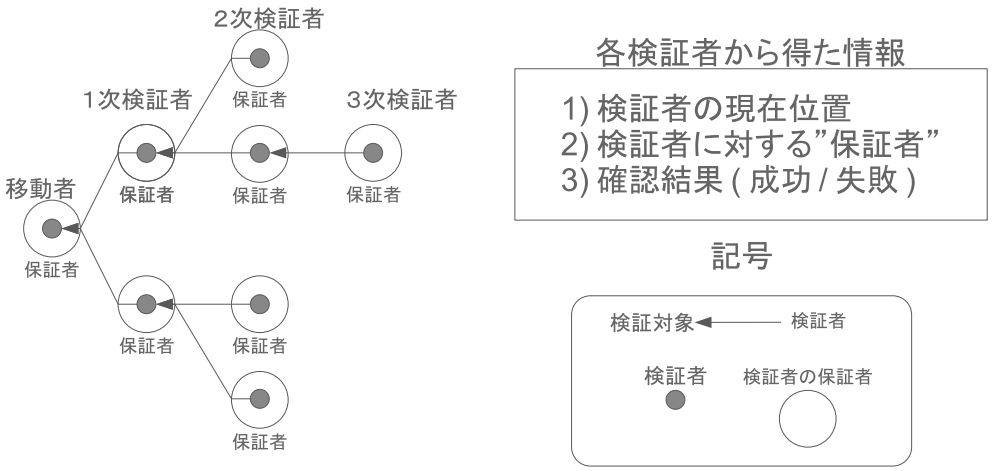

図 4.4: 要求者が得られる情報 (D=3 の例)

4.7 指標値の計算方法

自己改ざんと結託者を検知するための指標値の計算方法を示す。

検証ツリーの修正

検証ツリーに対して、指標値を求めるための修正を行う。まず、$i-1$ 次検証者を検証している i 次検証者との地理的距離を確認する (各検証者は、検証を行った時の現在位置を要求者に送信している)。このとき、$i-1$ 次検証者を検証した i 次検証者との地理的距離が無線 LAN の最大電波到達距離 r_{max} 以上なら、i 次検証者の検証結果を無条件に失敗に変更する。

検証結果が成功なのに、r_{max} 以上の地理的距離が生じる理由に、i 次検証者が嘘の現在位置を通知していたことが考えられる。これは、i 次検証者の実際の位置が $i-1$ 次検証者周辺で、i 次検証者が嘘の位置情報を送信していた場合におこる。

次に、自分の検証者を持たない i 次検証者 (検証ツリーの葉にあたる検証者) に対して、α^{D-i} $(\alpha \leq 1.0)$ の重み係数を設定する[2]。D は検証ツリーの深さである。最後に、各検証者の検証結果を、成功の場合 1、失敗なら 0 と置く。$D=3$ のときの修正後の検証ツリーの例を図 4.5 に示した。

指標値の計算

本計算方法では、最初に深さ D の検証ツリーで最も移動者から遠い D 次検証者の検証結果を元にして、$D-1$ 次検証者の “存在の確からしさ” を求める。以後同様に、i 次検証者から $i-1$ 次検証者の “存在の確からしさ” を後方伝播的に求めていき、最終的に移動者の “存在の確からしさ” を指標値として得る。

$n-1$ 次の検証者の “存在の確からしさ” は、各 i 次検証者の確認結果 $(1/0)$ と重み α を掛けて、相加平均を行うことで求める。このとき、深さ D 未満の、自分の検証者を持たない検証者の重み α は、深さ D の検証者に比べて小さく設定されている。これは、深さ D 未満の検証者に、深さ D の検証者と同じ重み α を与えると、相対的に深さ D 未満の保証者の結果の方が、指標値への影響が大きくなってしま

[2]設計では $\alpha=0.8$ を採用した

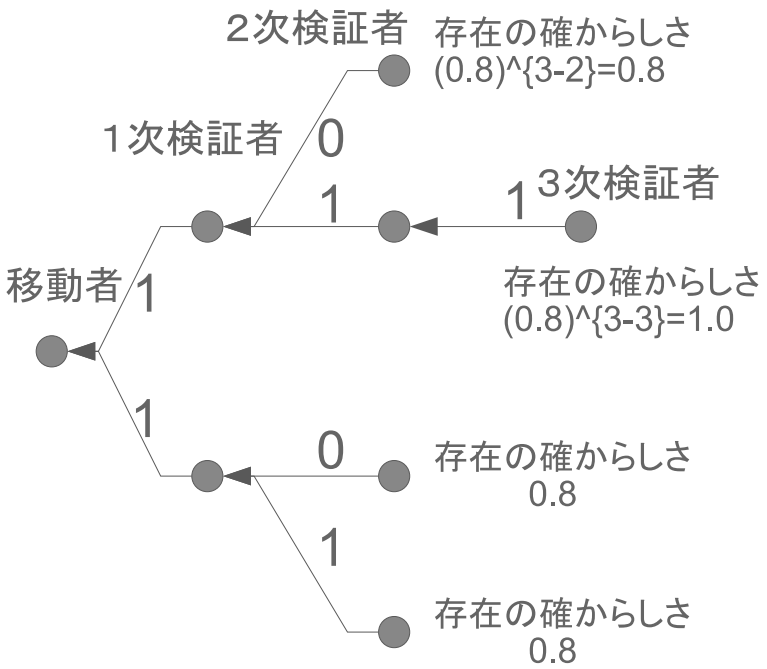

図 4.5: 修正後ツリー (D=3)

うためである。重み α の深さによる修正は、指標値への各検証者の影響を正規化するために必要である。指標値がとりうる最大値は検証ツリーによって異なる 1.0 未満の数値で、1.0 に近いほど移動者の位置情報の信頼性は高い。図 4.6 に $D = 3$ の場合の指標値の計算例を示す。

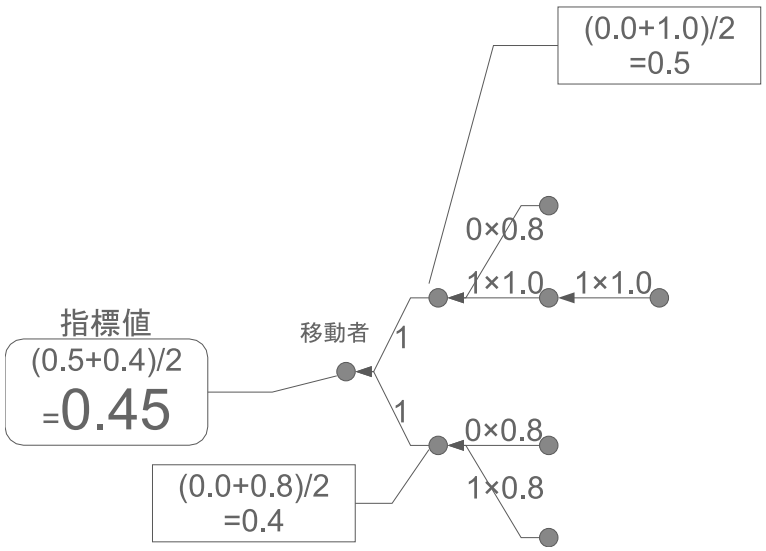

図 4.6: 指標値の計算例 (D=3)

4.8 シナリオ

ここでは、具体的なシナリオに沿って検証手順を詳しく説明する。

1. 要求者は移動者に対して、保証者を要求する

   (a) 移動者が $Geo(x, y)$ を自己改ざんしていない時 : 移動者は無線 LAN で周囲の第三者に保証を依頼する (図 4.7)

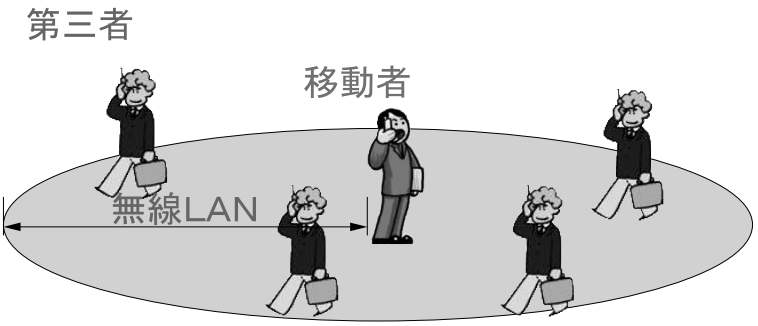

図 4.7: 保証者要求 (通常)

(b) 移動者が $Geo(x, y)$ を自己改ざんしていた時：移動者は嘘の保証者の一部を選んで、保証者となるように依頼する (図 4.8)

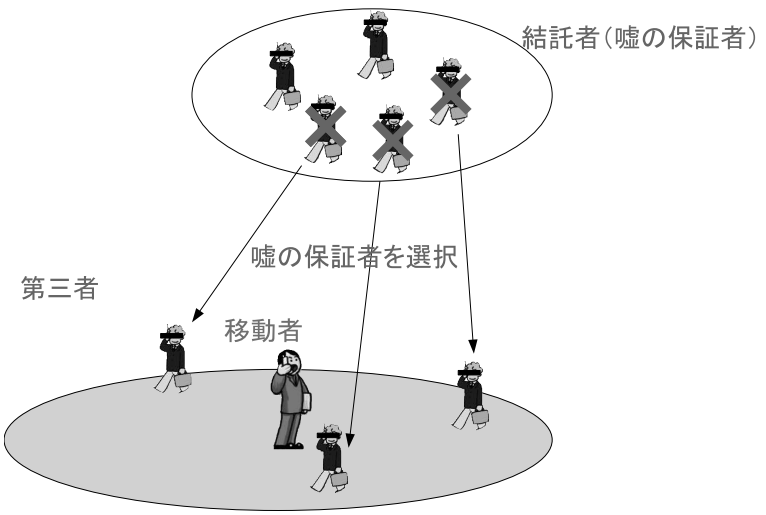

図 4.8: 保証者要求 (自己改ざん)

2. 移動者から依頼された保証者は、自分の ID を要求者に送信する

(図 4.9、図 4.10)

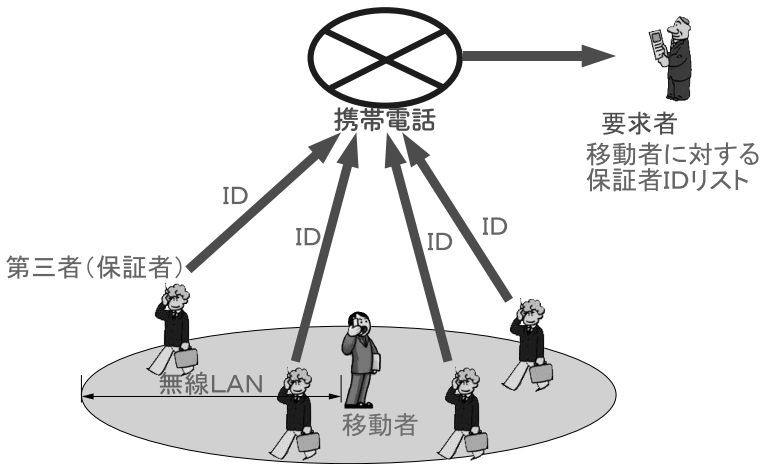

図 4.9: 保証者応答 (通常)

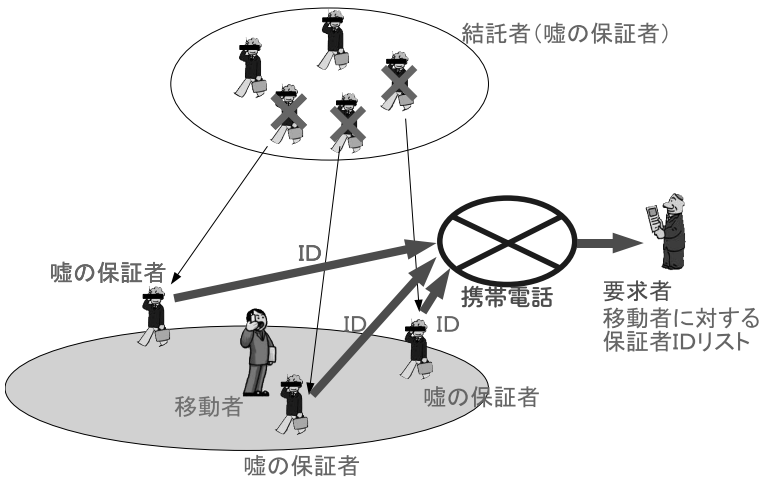

図 4.10: 保証者応答 (自己改ざん)

3. 要求者は保証者の中からランダムに複数の検証者を選ぶ。

   - 条件：すでに検証者となった保証者は選ばない。また、条件を満たす保証者がいない場合は終了。

4. 各検証者は、移動者を確認する

   (a) 検証者が結託者でないとき：移動者を無線 LAN を使って直接確認をする

   (b) 検証者が結託者であるとき：確認を行わない

5. 各検証者は検証結果を要求者に送る

   (a) 検証者は嘘の検証者でない：確認結果 (成功 / 失敗) と、現在位置を要求者に送信 (図 4.11)

   (b) 検証者は嘘の検証者である：確認結果は常に成功とし、$Geo(x, y)$ 周囲の適当な位置を送信 (図 4.12)

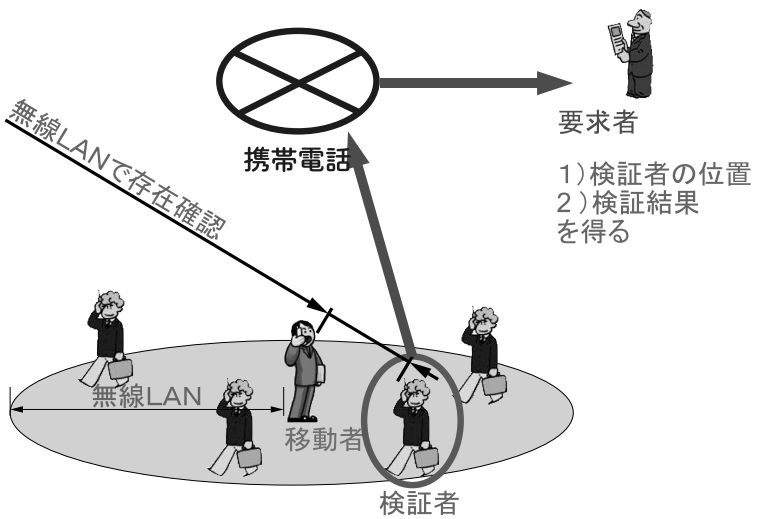

図 4.11: 検証実行 (通常)

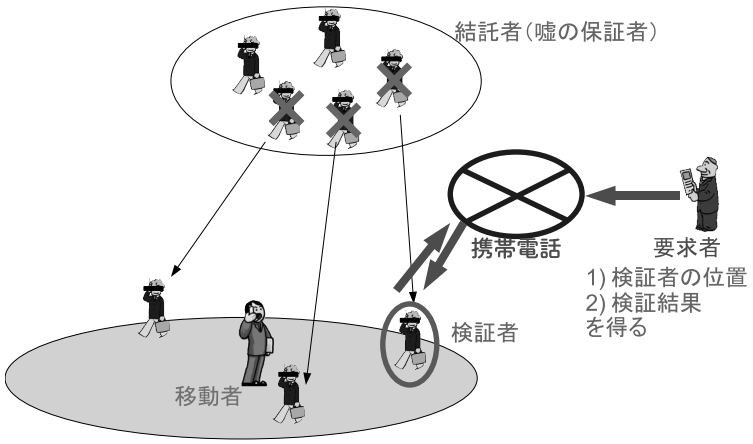

図 4.12: 検証実行 (自己改ざん)

6. 移動者 = 各検証者と再定義して、終了条件が満たされるまで、検証手順を繰り返す (再帰的な実行)(図 4.13、図 4.14)

   - 終了条件 1 : 手順を繰り返した結果、事前に設定した人数以上の保証者数を得た
   - 終了条件 2 : あたらしい保証者が得られない

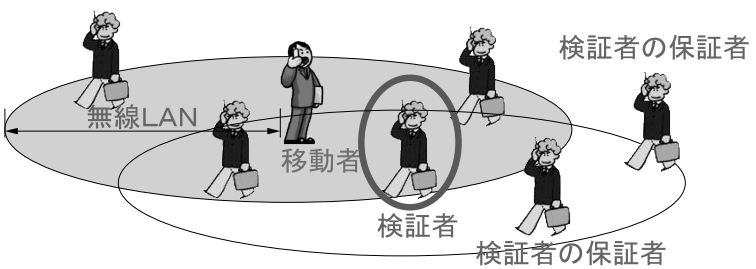

図 4.13: 保証手順繰り返し (通常)

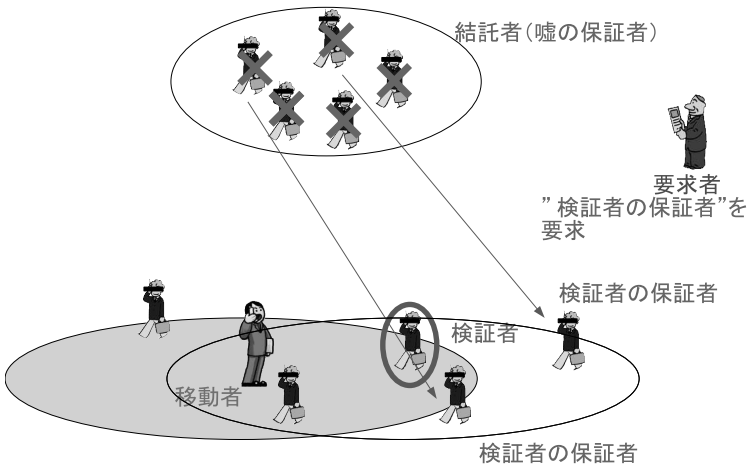

図 4.14: 保証手順繰り返し (自己改ざん)

結託者は結託者を自らの保証者、検証者にする必要がある。このため、多数の保証者を獲得すれば、結託者が枯渇する可能性が高まる。

結託者が枯渇した場合、結託者を利用していた移動者の行動は次の 2 つのどちらかである。

1. 新しい保証者が獲得できないことにする

2. 結託者以外の第三者を保証者とする

1. から、少数の保証者をえた移動者の位置情報よりも、多数の保証者がえられた移動者の位置情報の方が信頼性が高いと言える。2. の場合、結託者以外の第三者は結託者の情報と矛盾する情報を要求者に与えるため、評価値に影響する。

4.9 結託者対策

本システムでは、保証者と移動者が結託した場合に正しい保証ができないという問題があるため、対策が必要である。本システムでは、実世界のユーザの性質を利用して結託者問題への対策を講じている。

4.9.1 結託者の最大数

本システムでは、実世界ユーザが以下のような性質をもとにして、結託者問題への対策を行う。

1. 移動者と第三者関係にある多数のユーザは、移動者の不正 (自己改ざん) に協力 (結託) をしない
   - 理由 1:第三者には、移動者と結託すると得られるメリットがない
   - 理由 2:社会的にも、結託のような不正を嫌う人間の方が多い
2. 移動者が結託者を多数獲得するのは困難
3. 移動者の自己改ざんに協力する結託者は固定メンバになる

上に示した実世界のユーザの性質から、移動者は簡単に新しい結託者を獲得できない。そこで、移動者が獲得しうる結託者の最大数 $P_{MAXBOGUS}$ を本システムでは仮定し、$P_{MAXBOGUS}$ 以下の結託者に対して有効な対策を講じる。

4.9.2 結託者の枯渇

嘘の保証者は、自らの保証者に嘘の保証者を用意しなければならない。このため、必要な保証者数が $P_{MAXBOGUS}$ を上回ると、嘘の保証者は枯渇する。一方、第三者は、移動者のより遠方までを周囲とすれば、多数の第三者を獲得し続けること

が可能である。しかし、移動者の持つ端末の無線 LAN の電波到達範囲は数十メートル程度に限られる。

そこで、移動者が直接獲得した保証者 (1 次保証者) を利用し、“ 1 次保証者の周囲のユーザ = 2 次保証者” を求める。 2 次以降も同様に繰り返し (i 次保証者の保証者となる $i+1$ 次保証者)、より遠方まで多数のユーザ ID を獲得する。この方法で $P_{MAXBOGUS}$ 以上の保証者を要求し、結託者の枯渇させる。$P_{MAXBOGUS}$ 人の結託者を使いきった移動者が、とりうる行動は、次の 2 つである。

1. 新しい保証者 P を送信しない
2. 結託者以外の第三者を保証者とする

4.9.3 周囲の第三者数

要求者は 4.2.4 節の前提条件 (歩行者密度の統計情報) より、実際の保証者数と統計とを比較できる。また、要求者が移動者に対して検証を繰り返し行い、保証者数の分布も比較することができる。

このため、移動者は自己改ざんした位置の統計的性質 (保証者数の期待値) を考慮して結託者を利用する必要がある。移動者が、歩行者密度が高いエリアに位置を改ざんする場合、期待値以上の多数の結託者 (保証者) が必要になる。期待値以下の結託者の場合、統計的性質を満たすことができず、移動者の位置情報の信頼性が低いと判断できる。このように、歩行者密度が高いエリアでは「保証者数の期待値が大きい」ことで、結託者問題に対抗する。

一方、歩行者密度が低いエリアに移動者が位置を改ざんする場合、少数の結託者 (保証者) で統計的性質を満たすことができてしまう。歩行者密度が低い場合、要求者は一定時間経過後に検証手順を繰り返し実行する。自己改ざんでない場合、前回の検証と異なる新しい保証者がえられる可能性は高い。一方、自己改ざんの場合は、繰り返し行われる検証手順ごとに新しい保証者 (結託者) が必要になるため、

結託者の枯渇が期待できる。歩行者密度が低いエリアでは、一定時間経過後に「検証手順を繰り返し実行する」ことで、結託者問題に対抗する。

4.9.4 結託者の戦略

移動者が結託者を自らの保証者とするとき、結託者の利用方法が重要となる。本節では、移動者がとりうる 2 つの戦略における、移動者にとっての長所と短所を示す。

- 集中選択
  - 検証の全ての保証者を結託者とする戦略。
    - 長所：全ての検証結果を変更できる。
    - 短所：多数の結託者が必要。
- 確率的選択
  - 保証者リストに結託者以外の第三者を混入する戦略。
    - 長所：結託者数以上の保証者リストを作成できるため、結託者の枯渇発生の先伸ばしができる。
    - 短所：本検証手順では、要求者が保証者リストからランダムに検証者を選ぶため、第三者が検証者として選択される可能性がある。このとき、移動者の位置を否定される。

第 5 章

シミュレーション

設計した検証手順をシミュレーション実験を行った。まず、検証手順の通常の性質を明らかにするために、結託者が存在しない状況でのシミュレーションを行った (本章 5.2)。次に、移動者が結託者をどのように利用するかを分類して、移動者が結託者を持つ状況でのシミュレーションを行った。

5.1 実験環境

待ち行列シミュレーションライブラリ SMPL[6] を用いて、実験用シミュレータを C 言語で作成した。シミュレータのソースコード行数は約 2000 行である。

5.1.1 実験空間

移動者を中心とした正方形の平面エリア $1000 \times 1000m^2(1$ 平方 $km^2)$ に、歩行者が一様分布している空間で実験を行った。空間中の歩行者の総数は、実験パラメータとして任意に設定可能である。歩行者総数とエリアの大きさより、空間内の歩行者密度が求められる。このとき、歩行者の分布は一様分布であるため、エリア内の歩行者密度は一定となる。

5.1.2 物理パラメータ

シミュレータで採用した物理的なパラメータ (ex. 無線 LAN の通信可能半径など) を以下に示す。

無線 LAN

- 通信半径：平均 $50m$、標準偏差 $10m$ の正規分布
- 到達遅延時間：平均 $2.0ms$ の指数分布

携帯電話

- 送受信遅延時間：平均 $20ms$ の指数分布

GPS

- 測位時間：$10ms$

5.1.3 通信手順

実装した検証の通信手順は、保証者をえるための **CHK** フェーズと移動者の検証を行う **VRFY** フェーズの 2 つのフェーズで構成される。通信シーケンスを図 5.1 に、シーケンス中の各手順の詳細を表 5.1 に示した。

CHK フェーズ

要求者が移動者に対して CHK_REQ を送信する。CHK_REQ を受信した要求者は、CHK_BRCAST を無線 LAN でブロードキャストして周囲の第三者に保証者となることを依頼する。CHK_BRCAST を受信した第三者は、端末 ID と受信した CHK_BRCAST の電波受信強度 $[dB]$ の 2 つを CHK_SEND で送信し、要求者は移動者に対する保証者リストに格納する。IEEE802.11b などのほとんどの無線 LAN

では、無線 LAN の端末で電波受信強度を得ることが可能である。電波受信強度からは、移動者と保証者のおおよその距離を求めることが可能で、VRFY フェーズで検証者の選択に利用する。

CHK フェーズは、要求者が CHK_REQ を送信してからの規定時間でタイムアウトする。これは、CHK_SEND を送信する保証者数が CHK フェーズ前に自明でないためである。タイムアウト後に移動者に対する CHK_SEND トークンを受信した場合、保証者には含めない。実験では、CHK フェーズのタイムアウト時間を 100ms とした。

CHK フェーズのタイムアウト後、検証を行う VRFY フェーズに移行する。

VRFY フェーズ

CHK フェーズで得られた保証者リストの中から、検証を依頼する保証者 (検証者) を要求者が選択して、VRFY_REQ を送信する。選択される検証者は、検証手順の再帰実行を繰り返す点で、移動者から中程度離れていることが望ましい。この理由は、各検証手順で既に保証者となったユーザは、検証者として選択しないためである。移動者に近い検証者が検証手順を実行すると、無線 LAN の到達範囲が移動者とほぼ同一であるため、新しい保証者をえることが難しく、再帰実行を継続できない。

そこで、CHK_SEND でえた電波受信強度から移動者とのおおよその距離を求めて、無線 LAN 平均到達距離の 3/4 以下で、3/4 に近い保証者 2 名を選択する。3/4 以遠の検証者を除く理由は、移動者から遠いために CHK_EXEC が無線 LAN で到達せずに、VRFY フェーズの検証に失敗する可能性が高くなるためである。無線 LAN 平均到達距離の 3/4 の距離にある検証者は、面積比で 42.6%の新しい無線 LAN 通信可能エリアを持つため、新しい保証者を獲得できる可能性が高い。

検証者は、無線 LAN で移動者との直接通信を試みる (VRFY_EXEC,VRFY_REPLY)。検証者は検証結果 (成功/失敗) と、検証者

自身の現在位置を VRFY_SEND で送信する。

VRFY フェーズは、要求者が VRFY_REQ を送信してから規定時間でタイムアウトする。タイムアウト後に、検証結果 (VRFY_SEND) を受信した場合は、データの格納を行うが、その検証者を再帰的な検証手順の対象とはしない。実験では、タイムアウト時間を 50ms とした。

表 5.1: 通信トークン

トークン	送信元	送信先	送信データ	処理内容
CHK_REQ	要求者	移動者	-	保証要求
CHK_BRCAST	移動者	保証者	-	保証依頼放送
CHK_SEND	保証者	要求者	保証者 ID, 電波強度	保証者応答
VRFY_REQ	要求者	検証者 (保証者)	移動者 ID	検証要求
VRFY_EXEC	検証者	移動者	-	実行
VRFY_REPLY	移動者	検証者	移動者 ID	応答
VRFY_SEND	検証者	要求者	結果 (OK/NG), 検証者位置	送信

5.2 基礎実験

通常の検証手順での (結託者が存在しない場合) 歩行者密度と保証者数や検証者数との関係を実験から明らかにする。

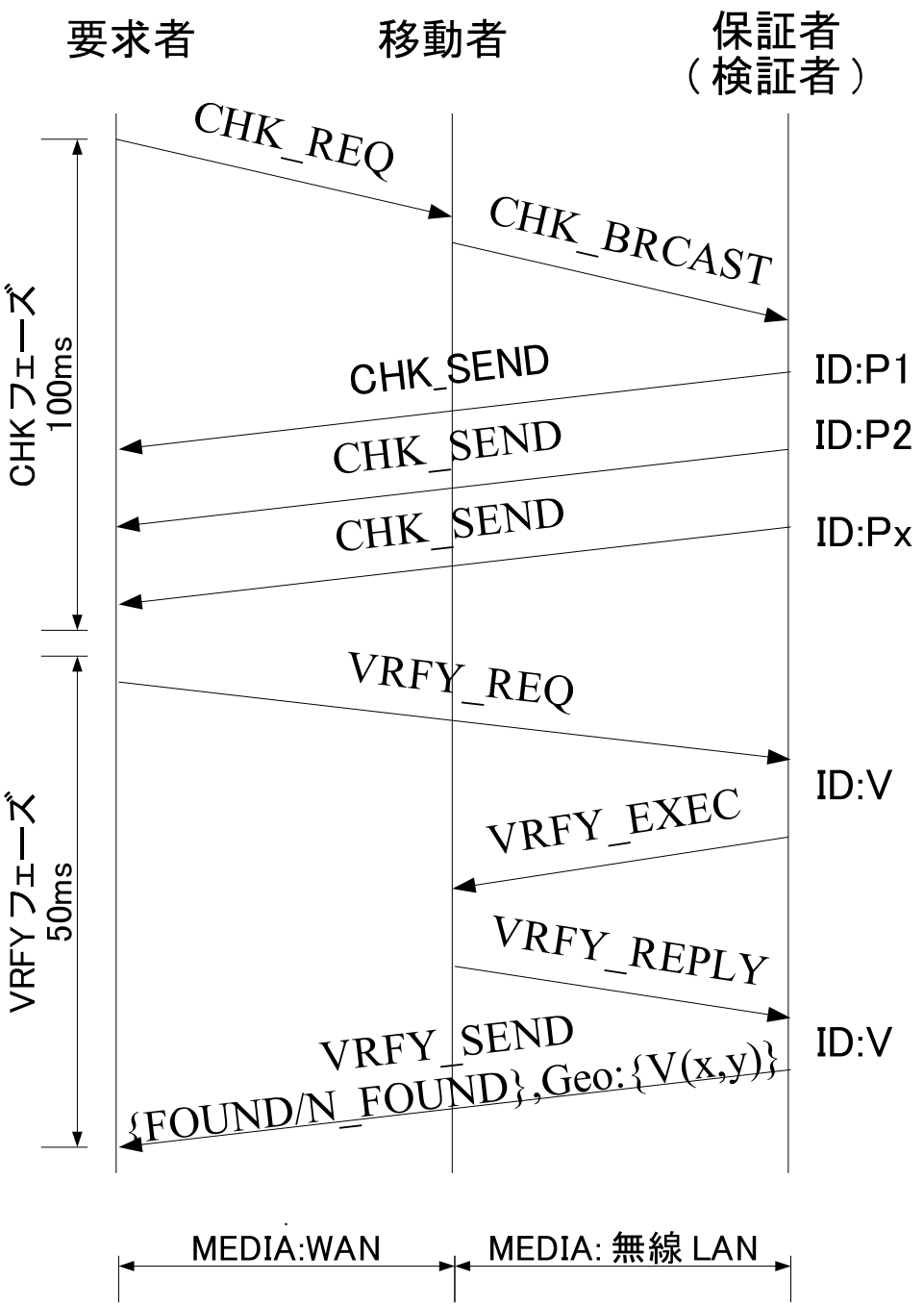
要求者
移動者
保証者
（検証者）
CHK_REQ
CHK_BRCAST
CHK_SEND
ID:P1
CHK_SEND
ID:P2
CHK_SEND
ID:Px
CHKフェーズ
100ms
VRFY_REQ
ID:V
VRFY_EXEC
VRFY_REPLY
ID:V
VRFY_SEND
{FOUND/N_FOUND},Geo:{V(x,y)}
VRFYフェーズ
50ms
MEDIA:WAN
MEDIA: 無線 LAN

図 5.1: 通信シーケンス

5.2.1 歩行者密度と保証者数

本検証手順では、実験空間内の歩行者数が多いときに (歩行者密度が高い)、多数の保証者を得ることができる。そこで、実験空間内の歩行者数と、検証終了時の保証者数と検証回数の関係をシミュレーションした。表 5.2 にその結果を示す。200 人 ~ 5000 人の各歩行者数ごとに各 500 回の検証を行って、得られた保証者数と検証回数を平均した。

シミュレーション結果より、歩行者数が 200 人 ~ 5000 人の範囲で検証者数は歩行者数に正比例していることがわかった。一方、平均保証者数は、最小二乗法を用いたて近似式を求めて、残差二乗和で適合度を比較した結果
2 次の近似式 $-0.89 + 0.0113x + 1.73 \times 10^{-6}x^2(x$=歩行者数) が最も適合した。本検証手順には、4.9 節で述べたように、移動者が嘘の保証者 (結託者) を用意して検証を回避する問題が存在する (結託者問題)。このとき、歩行者密度と保証者数の対応関係から、歩行者密度に対して必要な結託者数は 2 次式で増加する。要求者は、保証者数の平均値以上の保証者数を検証の基準として設定するため、自己改ざんを行う移動者は保証者の平均値以上の結託者を用意しなければならない。一方、4.9 節で述べたように、移動者が多数の結託者を用意することは一般に困難である。

このため、移動者は歩行者密度の低いエリアに位置情報を自己改ざんすることが多いと考えることができる。歩行者密度の低いエリアは、保証者数の期待値が小さいため、移動者の持つ結託者数で検知を回避できる可能性がある。このため、本検証手順では、歩行者密度が低いエリアでは、一定時間経過後に検証を繰り返し実行する。以前の検証でえられた保証者との集合和を作り、全体の保証者数を増加させることで、必要となる結託者は増えていく。検証を繰り返すことで、保証者数の期待値は、歩行者密度が高いエリアと同様になる。

従って、本研究では歩行者密度が高い状況を中心にして実験と考察を行った。

表 5.2: ユーザ数と保証者数

歩行者数/平方 km^2	平均保証者数	平均検証者数
200	2	1
500	5	2
800	9	3
1000	11	3
1200	14	4
1500	19	5
2000	28	6
2500	37	7
3000	49	9
4000	74	11
5000	98	13

5.3 改ざん検知実験

本検証手順の前提条件 (4.2.4 節) より、要求者は移動者の位置情報から歩行者密度 (本実験では 2000 人/平方 km^2) 知ることができる。これより、歩行者密度から求まる統計的性質と、実際の検証で得られたデータの 2 つを比較・評価することができる。また、歩行者密度の統計情報は公開情報なので、自己改ざんした位置の周囲の歩行者密度を、改ざんした移動者が知ることできる。このため、移動者は、歩行者密度から求まる平均保証者数などの統計的性質を満たすように結託者を使用しようとする。

移動者が結託者を用いて自己改ざんの検知回避を試みるとき、結託者の利用方法が 2 方法あることを 4.9.4 章で示した。

本章では、歩行者密度が 2000 人/平方 km^2 で移動者が結託者を一回目の検証から順に充填していった場合 (集中使用) と、確率的に充填する場合 (確率的使用) の 2 つの場合の各々で、改ざん検知の実験と考察を行った。

5.3.1 実験 1:結託者の集中使用

移動者が十分な結託者を持たずに、一回目の検証から順に結託者を保証者として充填していった場合 (集中使用) の検知を行う。このとき、移動者がもつ結託者数と、平均検証者数から得られる保証者数の累積比から、結託が行われている確率を求める。

まず、移動者の位置情報から求めた周囲の歩行者密度 (2000 人/平方 km^2) と分布状況 (一様分布) の 2 つを設定した 500 回のシミュレーションを行い、平均保証者数などを求めた (表 5.3)。これらの結果から、歩行者密度 2000 人/平方 km^2 では再帰的な検証の適用によって、平均して 6 人の検証者と 28 人の保証者が得られることが分った。次に、検証者数 6 人 (平均検証者数) でえられた保証者数の分布を図 5.2 に示す。図 5.2 の保証者数の最小値は 4 人、最大値は 62 人で平均値は 28 人

だった。さらに、図 5.2 を保証者数の累積比で表したのが図 5.3 である。

図 5.3 は、歩行者密度 2000 人/平方 km^2 で検証者数=6 人のとき、得られた保証者をパラメータとした「検証データ (位置情報) を信頼できる確率」のグラフと見ることができる。これは、移動者は多数の結託者を用意するのが困難であるため、要求者には少数の保証者数が得られる場合が多いと考えられるためである。このとき、えられた保証者数が 10 人、30 人だった場合、10 人のときの検証データの信頼性 (位置情報) は 4%、30 人では 68%と見ることができる。

表 5.3: 基礎実験での統計データ (歩行者密度 2000 人/平方 km^2)

項目	数値
平均検証者数	6 人
検証者の標準偏差	12.5
平均保証者数	28 人
保証者の標準偏差	17.2

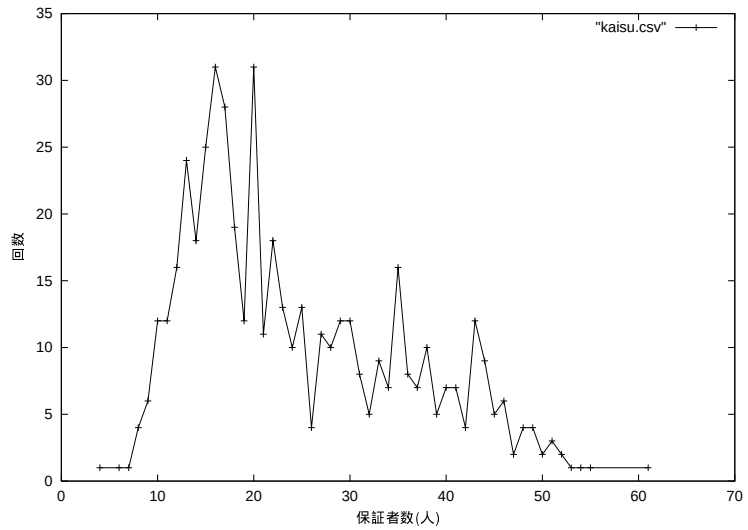

図 5.2: 保証者数 (密度 2000 人/平方 km^2, 検証者数 ≤ 6)

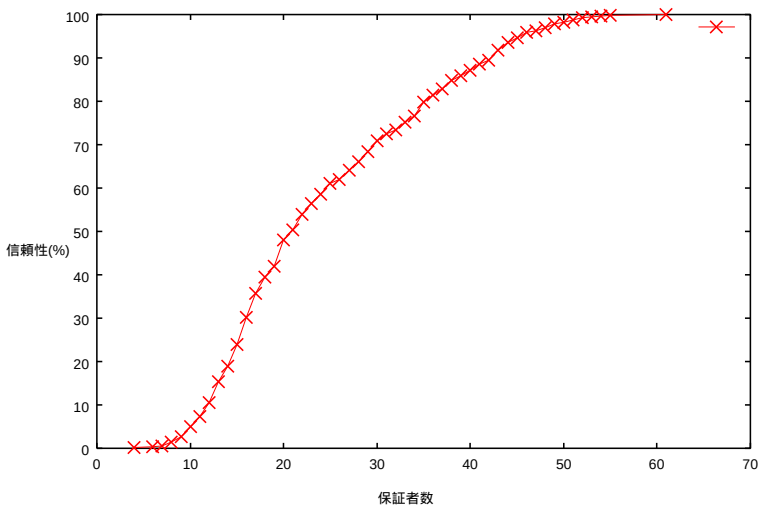

図 5.3: 保証者数の累積比 (密度 2000 人/平方 km^2, 検証者数 ≤ 6)

5.3.2 実験 2:結託者の確率的使用

移動者が、ある歩行者密度の期待値以上の結託者数 (保証者数) を持たない場合、保証者に結託者以外を混入して、枯渇を先伸ばしする戦略をとると考えられる。本検証手順では、保証者の中から検証者を要求者がランダムに選ぶ。このため、結託者から選ばれ続ける可能性 (確率) がある。

本実験では平均保証者数と同じ 28 人の結託者を持つ移動者が、保証者リスト中の 20% ~ 90%を結託者、残りを第三者として応答を行った時の指標値をシミュレーションした (実験回数 500)。各々の指標値の度数分布を図 5.4 ~ 5.7 に示した。指標値は、0.0 に近いほど位置情報の信頼性が低いことを示している。また、20% ~ 90%の各指標値を累積比を比較したのが図 5.8 である。

このとき、結託者数が 28 人が 20% ~ 90%の割合で保証者に含まれている場合、要求者が 80%の確率で改ざんを検知するには、図 5.8 から指標値 0.85 以上を判断の基準値とする必要があることがわかる。

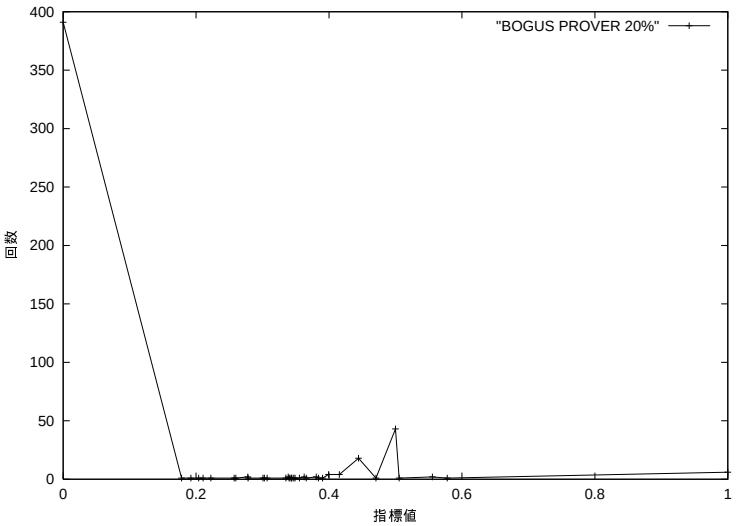

図 5.4: 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 20%結託者)

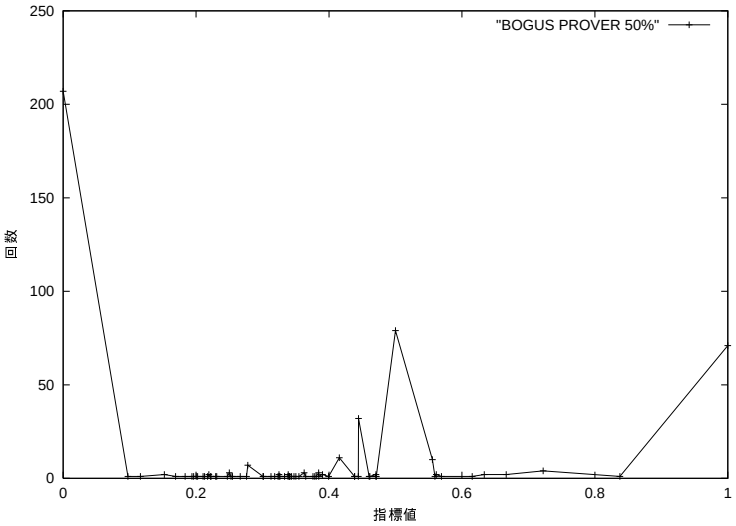

図 5.5: 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 50%結託者)

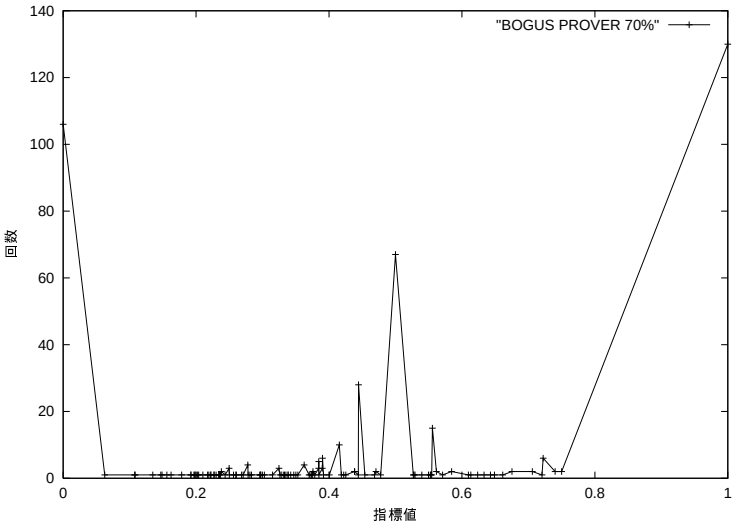

図 5.6: 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 70%結託者)

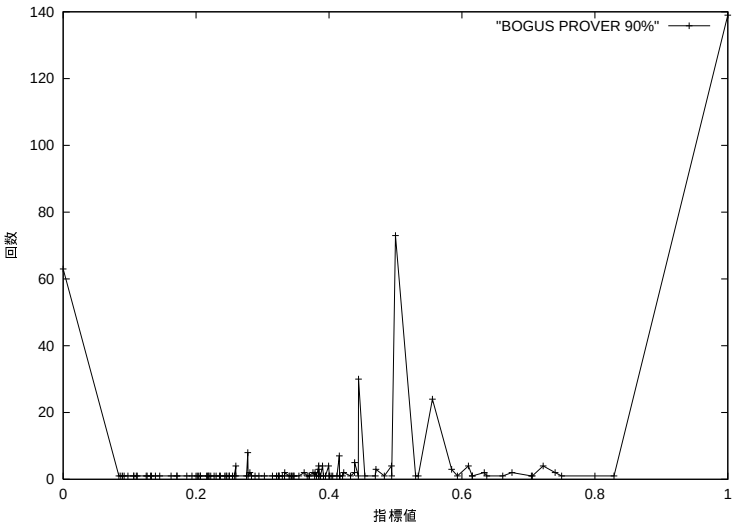

図 5.7: 指標値分布 (密度 2000 人/平方 km^2, 結託者数 28, 90%結託者)

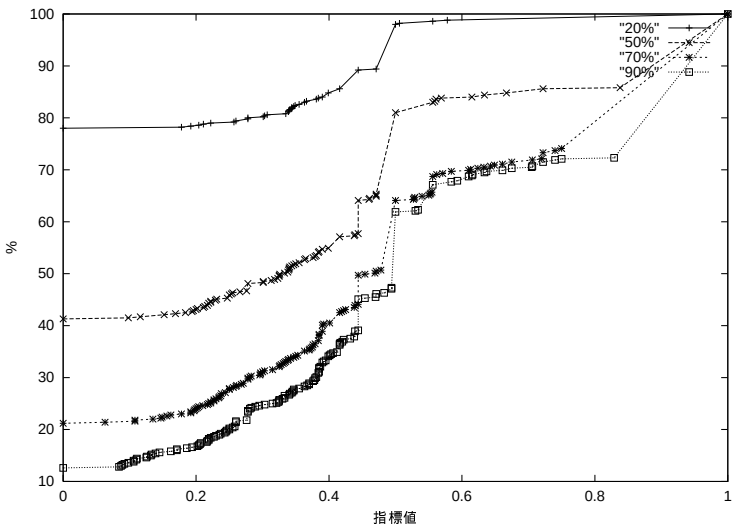

図 5.8: 指標値比較

第 6 章

問題点と課題

6.1 端末 ID 収集の問題

本システムでは、収集された端末 ID と位置情報の扱いの問題がある。本システムでは、端末 ID と所有者の対応関係が保たれていることを前提としている。検証の結果得られた保証者 P の端末 ID と位置情報から、所有者個人と位置が特定できるため、検証に使用した情報は、個人のプライバシに属する情報でもある。このため、周囲の第三者の位置情報を収集・利用する目的で本システムを用いられる可能性がある。しかし、位置情報の収集目的での検証手順実行を、現在の方法では防止することができない。

このような問題に対して、関連研究 2.1.5 GLI システムの発展研究で提案されている端末 ID 匿名化機構の応用が有効と考えている。GLI システムの拡張システム [7] では、ID の匿名化をハッシュサーバを用いることで実現している。匿名化サーバでは、一定時間 T ごとにハッシュ関数を変更して、受信した ID を変換する。端末が ID を送信するとき、匿名化サーバを中継させることで、受信者がユーザの本当の ID は得られないようにする。本システムでの平均検証時間よりも T を大きく設定すれば、検証実行中に得られるハッシュ化された ID は一意であり、本システムでの検証に問題はない。

6.2 過去データとの比較による改良

移動者 M の過去数回の保証手順でえた保証者のログ L_i を、要求者 R で記憶しておく。そして、新しく M の位置保証を行うときに、過去の保証者 ID と今回得られた保証者 ID の一致数を求める。エリアや時間が異なれば、同じ保証者 (ID) が得られる確率は小さい。そこで、$P_{MAXBOGUS}$ 以上の一致数があった場合、結託があったと判断する。

6.2.1 ID 一致数

各保証者ログ L_i は次の 3 つの情報から構成され、要求者 R が記憶している。

1. $Time_i$: 保証実行時刻
2. $Geo_M(x_i, y_i)$: 移動者 M の送信した位置
3. P_i : えられた保証者 ID リスト

新しく保証者リスト L_{now} が得られ、過去の保証者ログ L_i があるとき、以下の手順で一致数を求める。

1. 要求者 R が制限時間パラメータ T_{min}、制限距離パラメータ d_{min} を設定。L_{now} と保証時刻と位置の両方が近い L_i を除外するのに用いる。
2. T_{min} 以上の時間間隔、かつ d_{min} 以上の位置距離をもつ P_i を P_{check} に追加。
   (a) $P_{check} = \phi$
   (b) FOR:(i=1,2,3,...,N)
      i. IF:$(Time_{now} - Time_i > T_{min}) AND (distance|Geo_M(x_{now}, y_{now}), Geo_M(x_i, y_i)| > d_{min})$
      ii. THEN:$P_{check} = P_{check} + P_i$

(c) END FOR:

3. P_{check} と P_{now} で一致した ID 数が $P_{MAXBOGUS}$ 以上のとき結託があったと判断

6.3 指標値の計算方法

現在の指標値計算方法には、各検証者がもつ保証者リストの大きさや、保証者リスト間の関係性を用いていない。このため、収集した保証者リストが、指標値のパラメータとして反映されていないという問題がある。そこで、保証者リストの性質が反映される計算方法も含む複数の計算方法の試案を提示する。これらの計算方法での改ざん検知の可能性は、将来的な研究課題である。

6.3.1 保証者を利用した指標値

各検証者の持つ保証者を利用して指標値を求める。まず、無線 LAN の最大電波到達距離 r_{max} と検証ツリーの深さ D から、移動者の位置 $Geo(x, y)$ を中心として半径 Dr_{max} の最大到達エリアを求める。そして、検証者が通知した現在位置と検証結果をもとにして、3 つのグループに検証者を分類し、それぞれのグループの保証者の集合和を定義する。

1. 最大到達エリアの外の検証者のグループ V_{out}
   - P_{out} ：V_{out} の検証者が持つ保証者の和集合
2. 保証者を経由して移動者まで到達可能なパスを持つエリア内の保証者のグループ V_{good}
   - P_{good}：V_{good} の検証者が持つ保証者の和集合
3. 保証者を経由して移動者まで到達可能なパスを持たないエリア内のグループ V_{bad}

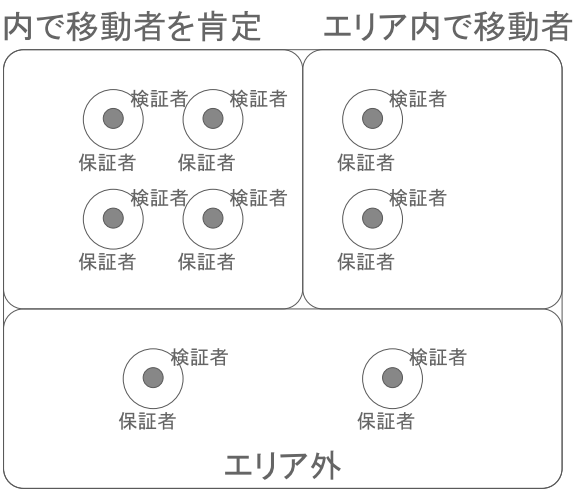

図 6.1: 位置によるグループ化

- P_{bad} ：V_{bad} の検証者が持つ保証者の和集合

まず、V_{out} に関して以下のことが言える。

- V_{out} に含まれる検証者は結託者ではない。
  - 移動者は自己改ざんの事実を隠すために、エリア内に結託者である検証者を配置するはずである。従って、V_{out} は結託者ではなく、V_{out} の情報は信頼できる。故に、V_{out} の持つ保証者 P_{out} も信頼できる。

V_{good} には結託者 (結託者問題) が、V_{bad} にはでたらめな結果を応答する検証者 (無確認問題) が含まれている可能性がある。そこで、V_{out} から得られた情報である P_{out} をもとにして、V_{good}、V_{bad} から疑わしい検証者を取り除く。

1. P_{out} と P_{bad} の両方に含まれる保証者を持つ v_{bad} をグループ V_{bad} から削除する。
   - v_{bad} がでたらめな保証者を送信している可能性がある。(無確認問題)
2. P_{out} と P_{good} の両方に含まれる保証者を持つ v_{good} をグループ V_{good} から削除する。

- v_{good} は結託者が枯渇して結果、結託者以外を保証者としたと推測できる。(結託者問題)

3. P_{good} と P_{bad} の両方に含まれる保証者を持つ v_{bad} と v_{good} は、どちらが正しいかわからない。よって、両方削除する。

   - V_{bad} が第三者なのか、無確認問題を持つでたらめな検証者なのかわからない。

最終的に得られた V_{out}、V_{good}、V_{bad} を以下の式に代入し、指標値を得ることができる。指標値の取りうる値の範囲は 0.0 から 1.0 までの間で、1.0 に近いほど位置情報の信頼性は高い。

$$\frac{V_{good}}{V_{out} + V_{good} + V_{bad}}$$

6.3.2 検証者の位置を使った指標値

無線 LAN の最大電波到達距離 r_{max} と深さ D から、移動者が自己改ざんを行っていない場合に無線 LAN で到達しうるエリアが求められる。そこで、移動者の通知した位置 $Geo(x, y)$ を中心として、半径 $D \times r_{max}$ のエリアを最大到達エリアと定義する。そして、検証者が通知した現在位置が最大到達エリア内に全て含まれているかを確認する。

もし、i 次検証者が通知した現在位置が最大到達エリア外であったなら、$i-1$ 次検証者以前に自己改ざんがあったと考えられる。最大到達エリア外に検証者の現在位置があることは通常の手順実行時にはありえない。そのため、移動者が結託者を検証者とする場合、最大到達エリア内に含まれるよう、検証者の現在位置を計算して通知するはずである。

このため、最大到達エリア外の i 次検証者は、何らかの理由で結託者以外が検証者となったと考えられる。従って、i 次以前の検証者に結託者が存在していると推定でき、移動者の位置情報の信頼性は低いと考えられる。このとき、全ての検証者

を V_{all}、エリア外の検証者数を V_{out} として、指標値は $1 - \frac{V_{out}}{V_{all}}$ で求める。指標値の取りうる値範囲は 0 から 1.0 までの間で、1.0 に近いほど位置情報の信頼性は高い。

第 7 章

おわりに

送信者自らが位置情報を改ざんして送信する自己改ざん問題の問題を提起し、従来の自己改ざん対策機構の問題点を分類した。従来は、特殊なハードウエアや外部環境に観測システムが必要であり、対策機構の構築にコストがかかっていた。

本研究では、これらの問題を踏まえて自己改ざんの検証手順を設計した。将来的に利用可能な汎用的な端末を用いて、周囲の第三者からの応答をもとに位置情報の信頼性を確認する検証手順を示した。また、設計した検証手順には移動者が第三者 (結託者) を用意して検証を回避する問題があるが、これに対する対策を検討しシミュレーション実験を行った。シミュレーションでは、移動者が結託者を利用する方法ごとに改ざんの検知確率を求めた。この結果、周囲の第三者密度にくらべて十分な結託者数を持たないときに、確率的に位置情報の自己改ざんを検知できることがわかった。

本研究でしめした自己改ざん検証手順は、全ての環境下で実行可能なわけではない。従来の自己改ざん対策も含めて、コストや用途、必要な保証レベルに合わせて選択可能な一つの選択肢である。今後の課題として、以下のことが挙げられる。

1. 結託者の利用方法によらない、最終的な位置情報の信頼性を示す指標値
2. 本研究の対策機構と他の対策との組み合わせ

謝辞

本研究を遂行するにあたって、いろいろな方々のお世話になりました。

まず、指導教官の多田好克先生からは日頃から熱心なご指導、そしてご鞭撻を賜わりました。そして、安田絹子助手からは研究方針や研究方法に多くの御指導をいただきました。お二人には、ご多忙中にもかかわらず論文の草稿を丁寧に読んで下さり、大変貴重なご助言をいただきました。ここに厚く御礼申し上げます。

そして、本研究を行なえたことは、共に研究生活をおくって様々な議論をすることができた多田研ならびに Vytas 研の学生諸氏のおかげでもあります。最後に、これらの皆さんに感謝いたします。

参考文献

[1] International Series Research,Inc. U.S Patent No.5,757,916 : Method and appartatus for authenticating the location of remote usets of networked computing systems, May 1998.

[2] Federal Communication Commission (United States). Common carrier bureau to hold ex parte meetings on wireline portion od enhanced 911 rule making. *PUBLIC NOTICE(DA-96-1463)*, No. 2, Sep 1996.

[3] 和泉順子, 竹内奏吾, 渡辺恭人, 植原啓介, 砂原秀樹, 寺岡文男, 村井純. 地理的位置情報システムにおけるプライバシ管理方法の提案. 情報処理学会マルチメディア、分散、協調とモーバイルシンポジウム論文集 (DICOMO '2000), pp. 667–672, Jun 2000.

[4] 竹内奏吾, 中村嘉志, 多田好克. インターネットにおける地理位置情報システムの設計と実装. 情報処理学会マルチメディア、分散、協調とモーバイルシンポジウム論文集 (DICOMO '99), pp. 405–410, Jun 1999.

[5] Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbon. The active badge location system. *ACM Transactions on Information Systems*, pp. 91–92, Jan 1992.

[6] M.H.MacDougal(小林 誠訳). シミュレーションによるコンピュータ・システムの性能評価:テクニックとツール. 工学社, April 1990.

[7] 渡辺恭人, 竹内奏吾, 寺岡文男, 植原啓介, 村井純. プライバシ保護を考慮した地理位置情報システム. 情報処理学会 論文誌, Vol. 42, No. 2, pp. 232–242, Feb 2001.

付録

構成要素の性質定義

ネットワークと端末

1. WAN ネットワークに送信する自分の端末 **ID** 以外の情報は、すべて送信側で変更・改ざんすることが可能である
2. 本システムの保証手順の要求が到着した端末は、基本的に端末内のプログラムで自動応答する
   (a) プログラムは、特定のユーザ ID の保証や検証の要求に対して、嘘の結果を返すように変更することが可能である

移動者

1. 移動者 $Mover, M$ は、正しい現在位置情報であることを証明する必要がある端末ユーザである

要求者

- 要求者 $Require, R$ は、位置情報の保証を必要としている位置情報システムやユーザである
- 要求者 R が、嘘の検証をしたり故意に嘘の情報を送信することはない
- 要求者は、想定端末を持たないがネットワーク (携帯電話) で地理的に離れた場所にいる、移動者 M、保証者 P、検証者 V と通信することが出来る

保証者

1. 保証者 $Prover, P$ は、移動者の周囲の端末ユーザであることを示すために、自らの端末 **ID** を要求者に送信したユーザの集合である
2. 保証者は P、嘘の保証者 P_{bogus} と真の保証者 P_{true} の 2 つの集合の和である
   $P = P_{bogus} \cup P_{true}$
3. 嘘の保証者
   (a) 嘘の保証者 P_{bogus} は、移動者 $Mover$ が位置情報改ざんに協力する端末ユーザである (第三者ではない)
   (b) 嘘の保証者 P_{bogus} の現在位置は、移動者 M の周囲にいるとは限らない
4. 真の保証者
   (a) 真の保証者 P_{true} は、移動者 M の改ざんに協力しない (第三者)
   (b) 真の保証者 P_{true} の現在位置は、移動者 M の本当の現在位置の周囲にのみ存在する

検証者

1. 検証者 $Verifier, V$ は要求者が得た保証者の中から選ぶ、保証者 P の部分集合である
2. 検証者 V とは、移動者 M の周囲の端末ユーザであることを示すために、自らの現在位置情報 $V_{Geo}(x, y, time)$ と端末 **ID**V_{id} を要求者 M に送信したユーザの集合である
3. 検証者 V の集合は、嘘の検証者 V_{bogus} の真の検証者 V_{true} の 2 つの集合の和である
   $V = V_{bogus} \cup V_{true}$

4. 嘘の保証者 V_{bogus}

   (a) 嘘の検証者 V_{bogus} は、嘘の保証者の集合 P_{bogus} の部分集合である

   $P_{bogus} \supseteq V_{bogus}$

   (b) 嘘の検証者 V_{bogus} は、移動者 M の自己改ざんに協力する検証結果を返す

5. 真の保証者 V_{true}

   (a) 真の検証者 V_{true} は、真の保証者の集合 P_{true} の部分集合である

   $P_{true} \supseteq V_{true}$

   (b) 真の検証者 V_{true} は、正しい検証結果を返す