

令和4年度 春学期 卒業研究3 (BI)
学士論文

題目 複数地域の Crowdsensing におけ
る最適ワーカサンプル法

指導教員 上山憲昭 教授

立命館大学 情報理工学部 セキュリティ・ネットワークコース

学籍番号 2600190334-8

松浦千紘

令和5年1月31日

概要

高性能のセンシング能力を搭載した携帯端末で計測したセンシングデータを、様々なワークから収集して真値を推定するモバイルクラウドセンシング (MCS: mobile crowdsensing) の利用が拡大している。

2010 年代にスマートフォンが広く普及してから、優れたセンシング機能を持ち合わせていることや広範囲から大量にデータを取得できること、インフラの構築が不要なため低コストであることなどからモバイル端末の IoT デバイスとしての活用が期待されており、特にセンサデバイスとしての MCS が注目されている。しかし、実際にはセンサで計測した値は誤差が生じていると予想され、MCS を用いたサービス事業者にとって誤差を抑制する方法の検討は必要不可欠である。

これまでの研究では、単一地域を対象としていた DPA 法を複数地域に拡張・適用し、推定誤差が最大となるように攻撃者を配置する方法などが提案されている。複数地域における推定誤差の抑制法については未検討であり、既存の研究では各エリアに存在している全ワークからデータを取集するが、サンプリングされたワークからデータを取集する方法については考慮されていない。本研究では、複数エリアのワークからデータを取集する際の、最適サンプル人数設定法を提案する。

目次

概要	1
第1章 序論	3
1.1 研究の背景	3
1.2 研究の目的	3
第2章 関連研究	5
第3章 既存方式	6
3.1 CRH 法	6
3.2 DPA 法	7
3.3 誤差を最大化する最適ポイズニング攻撃	8
第4章 CRH 法の精度の検証	9
第5章 提案方式	11
5.1 概要	11
5.2 最適化目標	12
5.3 アルゴリズム	13
第6章 性能評価	14
6.1 評価条件	14
6.2 複数エリアのサンプリング数調整に伴う総誤差の変化	15
6.3 総サンプルワーカー数を変化	16
6.4 標準偏差とエリア数を変更	17
第7章 まとめ	18
謝辞	19

第1章 序論

1.1 研究の背景

モバイル機器が一般に広く普及してから，モバイル機器に搭載されているセンシング能力がIoT デバイスを利用したセンシングの代わりとして注目を浴びている．IoT デバイスを利用したセンシングでは，公共の場に設置するためのコストや台数制限がかかるという問題があげられているが，普及率が高く新しくインフラを設置する必要のないモバイル機器を利用したセンシングの活用はこれを解決する．その他にも，モバイルクラウドセンシング (MCS: mobilecrowdsensing) の利点としては高性能のセンシング能力を搭載しており，様々な種類のデータを収集可能であるという点や，広い範囲での大量のデータ収集を得意とすることなどが挙げられる．

しかし，MCS の不特定多数からデータを収集するという特徴によって，収集データに矛盾が発生するといったデメリットがある．データを記録したり送信する過程で機器の誤作動などセンサの不具合や，ヒューマンエラーによる誤った測定値の送信が起きることで収集先の推定値に影響を及ぼすといった問題が発生している．特に，意図的に真の値から外れた値を送信し推定値を歪ませる悪意のあるワーカーが存在し，この攻撃は一般的にデータポイズニング攻撃と呼ばれている．

このデータポイズニング攻撃に対して推定誤差を抑制するために，ワーカーごとに報告値と推定値との差異に基づく信頼性を推定し，信頼性を重みとした報告値の加重平均を推定値に用いる CRH (Conflict Resolution on Heterogeneous data) 法が提案されている [1]．また，この CRH 法を活用して，悪意のあるワーカーがより推定誤差を大きくするように報告値を設定する DPA (Data Poisoning Attack) 法が提案されている [2]．

このようにワーカーからデータを取集する際，実際にはインセンティブの提供が必要であり，MCS の予算制約から一定の確率でサンプルされたワーカーからのみ推定値計算を行うことが予想される．

1.2 研究の目的

CRH 法 [1] と，DPA 法 [2] はいずれも単一エリアで適用可能なアルゴリズムである．複数エリアでの攻撃法について，攻撃ユーザ数を固定しこの DPA 法を複数エリアに適用，全エリアの推定誤差の最大化を目的として効率的な配置方法を提案したものがある．これらの研究は各エリアに存在している全てのワーカーからデータを取集するという想定のもと提案されているが，未だ複数地域でのサンプリング人数を考慮した誤差抑制法は確立されていない．

本稿では複数エリアでの MCS サービスを想定し，測定値を収集するワーカ数を固定したときの，総誤差の最小化を目的としたサンプリング人数設定アルゴリズムを提案する．

第2章 関連研究

これまでに、MCS サービスへのデータポイズニング攻撃方法や、それに対する防御法などが様々な観点から提案されている。

攻撃方法を提案している研究をいくつか紹介する。気温や湿度などの連続量を扱う MCS サービスを想定した研究に、MCS で送信される正常ワーカの報告データを観測し、攻撃者のデータパターンと似たパターンの正常ワーカデータに malicious データを加算することで検知される確率を下げるという特徴を持つ Poisoning 攻撃がある [3]。また Miao らは、複数の各オブジェクトに対し、カテゴリ選択型のデータを複数のワーカから集め、各オブジェクトの真のカテゴリを推測する場合に、ワーカの信頼度に応じた重みを考慮する Dawid-Skene モデルをクラウドが用いている場合の攻撃者の最適攻撃法を提案している [4]。さらに Miao らは複数の各オブジェクトに対し、カテゴリ選択型のデータを複数のワーカから集め、各オブジェクトの真のカテゴリを推測する場合に、(1) 推測結果の誤差を最大化、(2) 設定したターゲットに推測結果を誘導、の二つのタイプの Poisoning 攻撃の最適攻撃法を提案している [5]。

また、防御方法を提案している研究に、Huang らの、複数の各オブジェクトに対し真値を推測する場合に、誤差最大化を目的とした Poisoning 攻撃者に対し、推測値からの誤差が閾値を超えたワーカを除外する提案がある [2]。複数のカテゴリから該当するものを選択する MCS を対象としたものとして、例えば Varshney は複数の報告値から多数決でカテゴリを選択する場合を対象とした Worker 間の結託に対する防御法を提案している [6]。

しかし、これらは単一のエリアにおける MCS サービスを想定しており、複数のエリアにおける MCS を対象とした研究ではない。これに対し、複数エリアでの MCS サービスを想定し、全てのエリアの誤差の最大化と、最も誤差の小さなエリアの誤差の最大化を目的とした攻撃ワーカの配置方法アルゴリズムを提案しているものがある [7]。

第3章 既存方式

3.1 CRH 法

CRH 法は、複数の情報源から真実を推測することを目的としたアルゴリズムである [1]. 推定値と入力データとの間の全体的な加重偏差を最小化する. その際にワーカごとの信頼性を推定し, 信頼性を重みとした測定値の加重平均を推定値に用いる. MCS に適用した場合, 測定値の推定値と報告値との差異が小さいワーカの信頼性は高く, 大きいワーカの信頼性は低くなるようにワーカの信頼性を設定する. 推定値とワーカごとの信頼性を交互に更新することで, 推定値と真値の差を最小化する. 以下に CRH 法のアルゴリズムを示す. ただし正常ワーカの集合を N とし, 攻撃ワーカの集合を A とする.

1. 各ワーカ k の信頼性 (重み) w_k を 1 に初期化
2. 式 (3.1) で, 各ワーカ k の報告値 v_k と w_k から, 推定値 $\tilde{v}$ を計算

$$\tilde{v} = \frac{\sum_{k \in N \cup A} v_k w_k}{\sum_{k \in N \cup A} w_k} \quad (3.1)$$

3. 式 (3.2) でワーカごとの信頼性 w_k を更新

$$w_k = -\log \frac{(v_k - \tilde{v})^2}{\sum_{k \in N \cup A} (v_k - \tilde{v})^2} \quad (3.2)$$

4. $\tilde{v}$ 及び w_k が収束するまで step 2, step 3 を反復

3.2 DPA 法

DPA 法は, CRH 法による推定値及びワーカごとの信頼性の更新ステップ, 攻撃ワーカの報告値の更新ステップの 2 ステップを繰り返すことで, 推定誤差を最大化する攻撃ワーカの最適報告値設定アルゴリズムである [2]. 攻撃者の最適化目標は, 正常ワーカのみで推定した値 $\hat{v}$ と, 攻撃ワーカを含めた全ワーカで推定した値 $\tilde{v}$ の絶対差を最大化することである. 単一エリアを対象とした DPA 法のアルゴリズムを以下に示す.

1. 各攻撃者 k の報告値 v_k の初期化
2. 正常ワーカのみで CRH 法を用いて推定値 $\hat{v}$ を算出
3. 全ワーカを対象に CRH 法を用いて推定値 $\tilde{v}$ を算出
4. 各攻撃ワーカ k に対し, 式 (3.3) で報告値 v_k を更新

$$v_k = v_k + 2 \times (\hat{v} - \tilde{v}) \times \frac{w_k}{\sum_{k \in N \cup A} w_k} \quad (3.3)$$

5. v_k が収束するまで step 3, step 4 を反復

3.3 誤差を最大化する最適ポイズニング攻撃

複数エリアの MCS サービスを対象とした最適データポイズニング攻撃法について、DPA 法を複数エリアに拡張したアルゴリズムに誤差の上限値と下限値を設定することで、総推定誤差の最大化と攻撃ワーカの分散配置の両立を実現する [7].

動作について示す. 全攻撃ワーカを未配置状態に初期化し, 未配置攻撃ワーカの中から仮配置攻撃ワーカ m を決定する. エリア s に仮配置し, DPA 法を用いて正常ワーカのみを用いて算出した推定値 $\tilde{v}_s$ と, 全ワーカを対象に算出した $\hat{v}_s$ を算出. その差分の絶対値をエリア s の誤差 e_s とする.

ここで, 各エリア s に誤差の上限値 η_u と下限値 η_l を設定する. 誤差上限法 ULM では, $e_s < \eta_u$ のエリアに攻撃ワーカを仮配置し, それを上回るエリアは攻撃ユーザ仮配置対象から除外する. $e_s < \eta_u$ のエリアの中で, e_s の増加量が最大となるエリアに攻撃ワーカを追加配置する. この処理を全てのエリアが上限値に達するまで反復する. 全エリアが上限値に達し, 未配置の攻撃ワーカが存在する場合, e_s の増加量が最大となるエリアに追加配置する処理を行う. 誤差下限法 LLM も同様に, $e_s < \eta_l$ のエリアに攻撃ワーカを仮配置し, それを上回るエリアは攻撃ワーカ仮配置対象から除外する. LLM では, $e_s < \eta_l$ のエリアの中で, e_s が最小となるエリアに攻撃ワーカを追加配置する. この処理を全エリアが下限値に達するまで反復して行い, 下限値に全エリアが達し, かつ未配置攻撃ワーカが存在する場合, e_s の増加量が最大となるエリアに追加配置する処理を行う.

このようにして全攻撃ワーカを配置し終わると, 処理を終了する.

上限値 η_u と下限値 η_l を変化量として与え, 各手法の総誤差 E と最小誤差 e_s の推移の様子を考察. 誤差上限法 (ULM) においては, η_u が小さい領域では, すぐに全エリアの e_s が η_u に達するため, 攻撃ワーカは e_s の増加量が大きなエリアに集中的に配置され, E が大きく e_{min} が小さい. また η_u の増加に伴い, より e_s の増加量が小さいエリアに攻撃ワーカが多く配分される結果, E は減少していく半面 e_{min} は増加し, 攻撃ワーカの偏りは減少する. さらに η_u を増加させていくと, 再度, より多くの攻撃ワーカを e_s の増加量が大きなエリアに割り当て可能となり, η_u の増加に伴い E が増加するが, e_{min} は減少し, 配置攻撃ワーカ数の偏りがより大きくなるといった傾向が見られた. 一方, 誤差下限法 (LLM) においては, η_l が小さい領域では, すぐに全エリアの e_s が η_l を上回るため, 攻撃者は e_s の増加量が大きなエリアに集中的に配置され, E が大きく e_{min} が小さい. また η_l の増加に伴い, より e_s の増加量が小さいエリアに攻撃者が多く配分される結果, E は減少する半面 e_{min} は増加し, 攻撃ワーカの偏りは減少する. さらに η_l を増加すると, より多くの攻撃ワーカが必要な e_s の増加量が小さなエリアに多くの攻撃ワーカを割り当てる. そのため η_l の増加に伴い E が減少するが, e_{min} が増加し, 配置攻撃ワーカ数の偏りも増加する. しかし, さらに η_l を増加させると E と e_{min} は η_l が変化しても一定となるといった傾向があった. これは, どのエリアも η_l の値に届かなくなり, 攻撃ワーカの配置状況が変わらなくなるためである.

正常ワーカ数が各エリアで異なる場合や, 正常ワーカの報告値の標準偏差がエリア毎に異なる場合なども同様の実験を行ったところ, いずれも η_l を 7~12 程度に設定した LLM が攻撃者にとって望ましい攻撃者配置法と考えられる.

第4章 CRH法の精度の検証

本節では，単一エリアを対象に CRH 法を適用し，正常ワーカー数の変化による推定誤差の推移の様子を観察する．実験条件として，エリア数を $k = 1$ ，正常ワーカーの測定値の平均を 50 に設定する．また，正常ワーカー数を $2 \leq n \leq 100$ の範囲で変化させ，推定誤差の推移を観察する．正常ワーカーの測定値の標準偏差を 20, 40, 60 のそれぞれの場合で比較し，評価には 1000 回の試行の平均値を用いる．

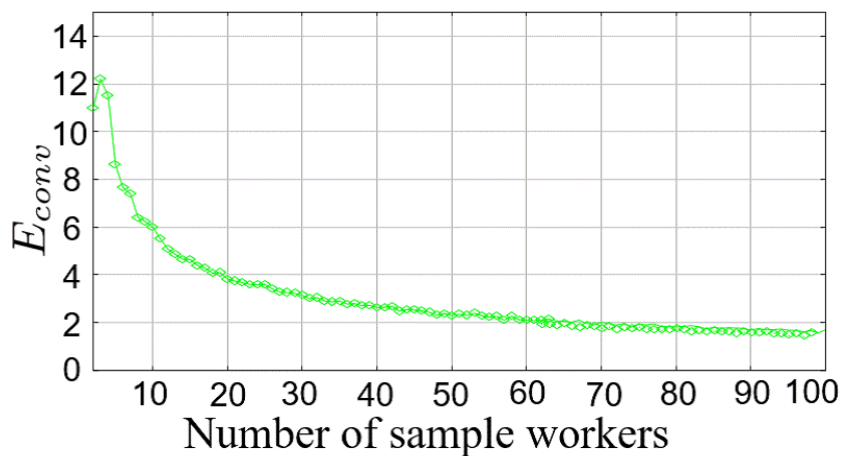


図 4.1: 正常ワーカーの測定値の標準偏差が 20 の場合

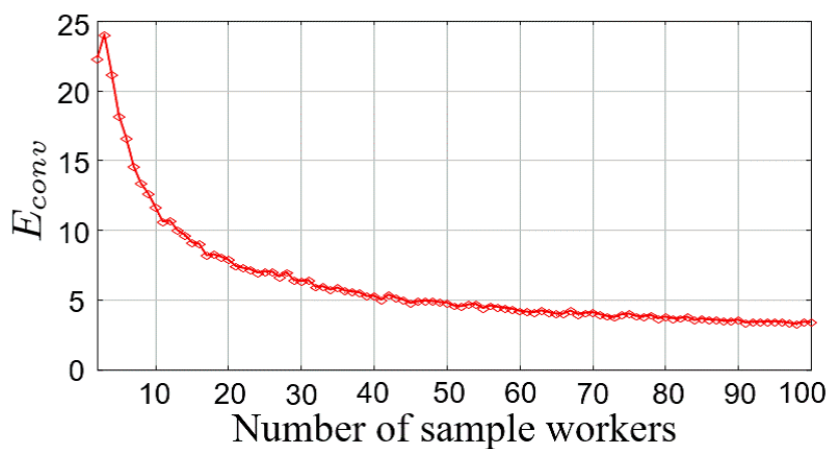


図 4.2: 正常ワーカーの測定値の標準偏差が 40 の場合

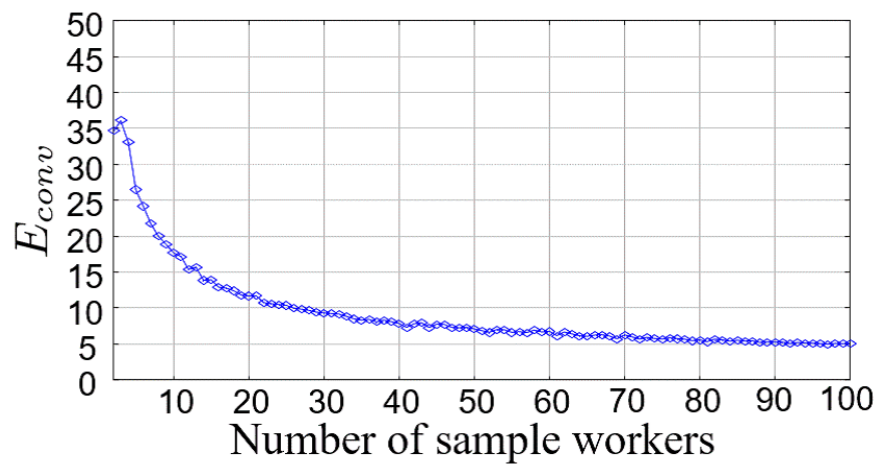


図 4.3: 正常ワーカーの測定値の標準偏差が 60 の場合

どの条件においても、正常ワーカー数の増加に伴い総誤差 E は単調に減少する傾向が見られる。縦軸の推定誤差の値を標準偏差別に観察すると、標準偏差の小さい、すなわち正常ワーカーの測定値のばらつきの小さいエリアほど推定精度が高いことがわかる。また、サンプルワーカー数の変化に注目すると、標準偏差の大きいエリアほどサンプリング数を増加させたときの推定誤差の変化量は大きい。

このように CRH 法を単一エリアに適用した場合、正常ワーカーの数が多く、測定値のばらつきが小さいほど推定精度が高くなる。この結果を利用して、複数エリアの MCS サービスにおいて総サンプルワーカー数が固定である場合の、総誤差の最小化を目的とした各エリアのサンプルワーカー数の最適化アルゴリズムを提案する。

第5章 提案方式

5.1 概要

MCS の運用者は，ワーカからデータの提供を受けるにはインセンティブをワーカに支払う必要があるので，総サンプルワーカ数の上限 N を制約条件として考慮し，本条件下で総誤差 E が最小となるよう各エリア i のサンプルワーカ数 u_i を最適設計する．第4章では，単一エリアで CRH 法を用いて正常ワーカの人数と推定誤差との関係性を示す実験を行った．この方式を特性の異なる複数エリアで同様に実験し，得られた数値を用いて提案方式であるサンプリング人数設計アルゴリズムを実行する．

5.2 最適化目標

MCS 運用者の最適化目標として、全エリアの誤差の総和 E の最小化を考える．提案方式で用いるパラメータを以下の表 5.1 に示す．

表 5.1: 提案方式に用いられるパラメータとその定義

記号	定義
K	エリア数
N	総サンプルワーカー数
u_i	各エリア i のサンプルワーカー数
p_i	各エリア i の測定値の真値
μ_i	各エリア i のワーカー報告値の平均値
σ_i	各エリア i のワーカー報告値の標準偏差
v_i	エリア i の推定値
E	総推定誤差
e_{i,u_i}	サンプルワーカー数 u_i の場合のエリア i の推定誤差
S_0	初期配置状態
S_1	サンプリング数最適化後の配置状態
η	総誤差の差分の判定に用いる閾値

エリア i の推定値を v_i 、真の値を p_i とすると、エリア i の推定誤差は $|v_i - p_i|$ となるので、全エリアの誤差の総和 E の最小化を目的とする目的関数を (5.1) 式で与える．また制約条件を (5.2) 式で与える．

$$\min E(u_1, u_2, \dots, u_K) = \sum_{i=1}^K (v_i - p_i)^2 \quad (5.1)$$

$$\sum_{i=1}^K u_i = N \quad (5.2)$$

5.3 アルゴリズム

各エリア i の測定値の平均を μ_i 、標準偏差を σ_i とし、以下のアルゴリズムで本最適化問題の近似解を得る.

1. データ収集する総ワーカ数を N 、各エリアの正常ワーカ測定値の平均を μ_i 、正常ワーカ測定値の標準偏差を σ_i 、エリア数を K とし、これらを入力値として与える
2. 各エリアのサンプルワーカ数を $u_i = N/K$ とし、これを初期配置状態 S_0 とし、このときの総誤差 E_{ini} を算出
3. 何回かランダムにサンプルワーカ数を与えたときの平均推定誤差を算出することで、各エリアのサンプルワーカ数に対する平均推定誤差 e_{i,u_i} のデータベースを作成
4. ワーカ数調整前の総誤差を E_{pre} とする. 各エリア i のサンプル人数をインクリメントしたときの平均誤差 e_{i,u_i+1} をデータベースから取得
5. 各エリア i のサンプル人数更新後の推定誤差の減少量 $e_{dec} = e_{i,u_i} - e_{i,u_i+1}$ を算出
6. 各エリア i のサンプル人数をデクリメントしたときの平均誤差 e_{i,u_i-1} をデータベースから取得
7. 各エリア i のサンプル人数更新後の推定誤差の増加量 $e_{inc} = e_{i,u_i-1} - e_{i,u_i}$ を算出
8. e_{dec} が最大となるエリアの u_i をインクリメントし、 e_{inc} が最小となるエリアの u_i をデクリメントし、このときの総誤差 E_{post} を算出
9. 総誤差の変化量 $|E_{post} - E_{pre}|$ が閾値 η を下回るまで、step 4 ~ step 8 を反復
10. step 9 の条件を満たしたとき (状態 S_1) の各エリアのサンプルワーカ数を最適サンプル人数とし、このときの総誤差 E_{conv} を算出.

第6章 性能評価

6.1 評価条件

性能評価で使用するパラメータを表 6.1 にまとめる.

表 6.1: 評価に用いたパラメータ

記号	値
K	10
N	400
μ_i	50.0
σ_i	2.0, 4.0, 6.0, 8.0, 10.0, 12.0, 14.0, 16.0, 18.0, 20.0
η	10^{-5}

各エリアの測定値の平均 μ_i を 50 とし, 各エリアの標準偏差を最小 2・最大 20 の 2 刻みで設定する. エリア数 10 個, 総サンプルワーカー数 400 人より, 提案方式を適用すると各エリアの初期配置ワーカー数は 40 人となる. 初期配置状態を S_0 と表し, S_0 の際の総誤差を E_{ini} , ワーカー調整終了時の総誤差を E_{conv} とする. ひとつ前の調整時に算出した総誤差を E_{pre} と表し, E_{post} と E_{pre} の差分の閾値判定に η を用いる.

本節では, 上記のパラメータを入力値として, 総誤差 E_{ini} から E_{conv} にかけての推移を観察する. また, 総サンプルワーカー数を変化させたときの総誤差 E_{ini} と E_{conv} の推移の様子もプロットし, 上記の入力値を用いた場合と, 標準偏差の幅とエリア数を変更したモデルとの比較を行う.

6.2 複数エリアのサンプリング数調整に伴う総誤差の変化

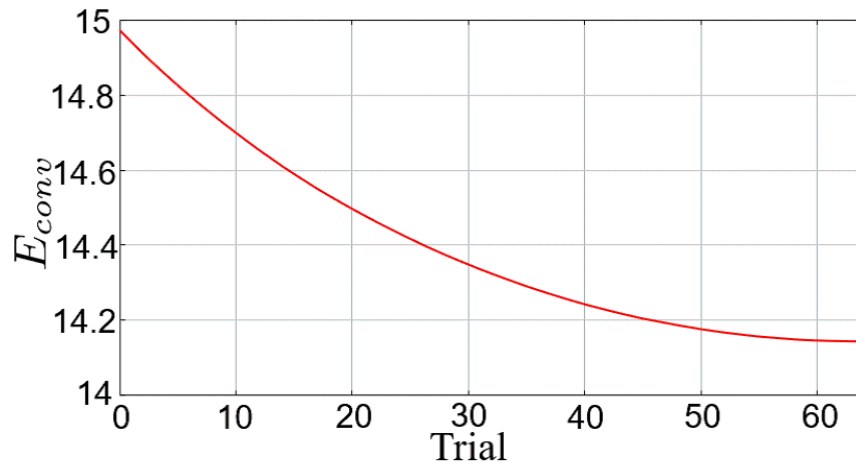


図 6.1: サンプリング数調整回数に伴う総誤差の推移

図 6.1 は、提案方式を用いたときの総誤差 E_{ini} から E_{conv} にかけての推移のグラフである。調整回数 (Trial) を重ねるにつれ総推定誤差は単調減少していることがわかり、初期配置状態 S_0 と比較して S_1 の状態の各エリアのサンプリング人数は推定精度を考慮したものとなっている。以下に状態 S_1 の各エリアのサンプリング人数を示す。

表 6.2: 各エリアの最終サンプリング人数

area	σ_i	サンプリング人数
1	2.0	13
2	4.0	23
3	6.0	28
4	8.0	34
5	10.0	39
6	12.0	44
7	14.0	48
8	16.0	53
9	18.0	57
10	20.0	61

表 6.2 を見るとワークの測定値の標準偏差が大きいエリアほどサンプリング人数が多くなっているが、数値のばらつきが大きいエリアほど推定精度が低いため、サンプリング人数を増加させることで推定精度の向上を図るためだと考えられる。

6.3 総サンプルワーカ数を変化

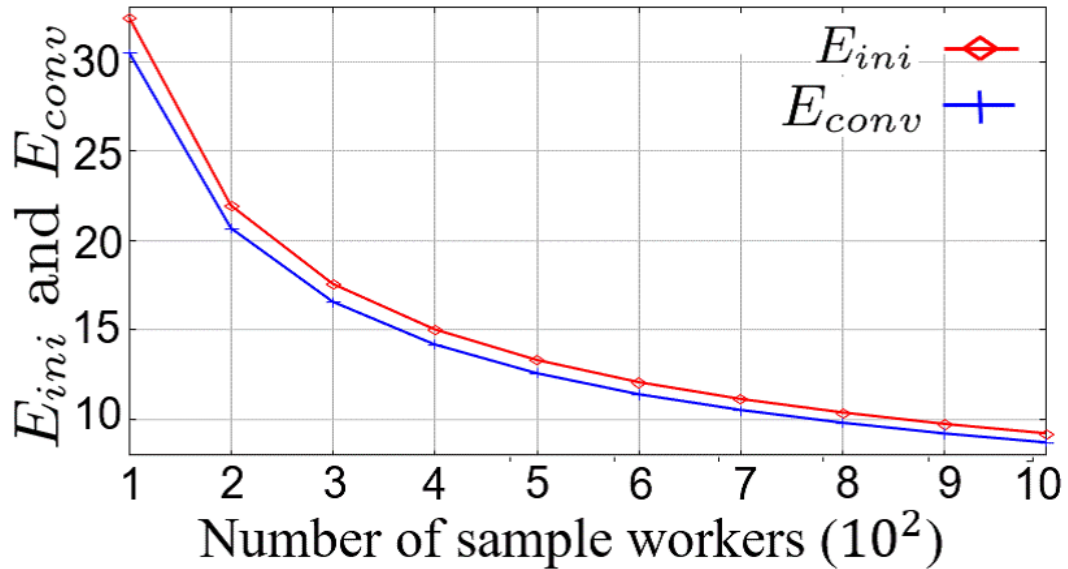


図 6.2: 総サンプルワーカ数を変化させた場合の総推定誤差の推移

図 6.2 は、総サンプルワーカ数を最小が 100，最大が 1000 の 100 刻みで設定したときの総推定誤差 E_{ini} と E_{conv} の推移を観察したものである．このときの実験条件を表 6.1 のように設定し，条件 A とする．総サンプルワーカ数による E_{ini} と E_{conv} の値の幅には大きな影響は見られなかった．しかし，総サンプルワーカ数を増加すると総推定誤差は単調減少し，推定精度は向上することがわかる．

6.4 標準偏差とエリア数を変更

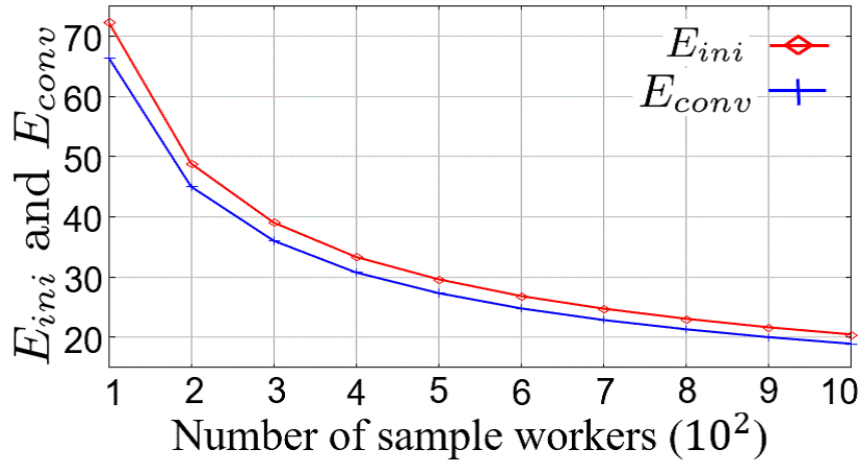


図 6.3: 標準偏差の幅を変更させた場合のサンプルワーカー数毎の総誤差

図 6.3 は、エリア数は同一で標準偏差の幅を図 6.2 の場合より大きく設定したときのグラフであり、この場合を条件 B とする。A の標準偏差を最小が 2，最大が 20 の 2 刻みで設定し、B の標準偏差を最小が 2，最大が 47 の 5 刻みで設定した。総推定誤差の値は、標準偏差の幅が大きくなるほど全体的に大きくなることが確認できた。

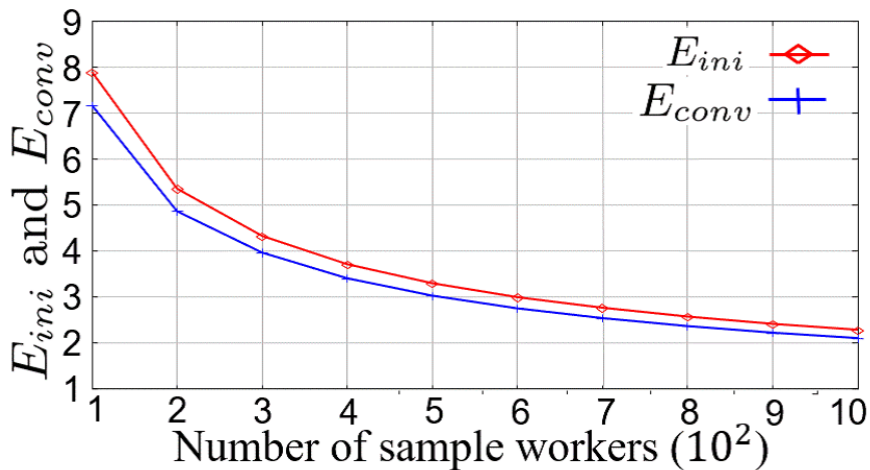


図 6.4: エリア数を変更させた場合のサンプルワーカー数毎の総誤差

図 6.4 は、標準偏差の幅は同一でエリア数を図 6.2 の場合より少なく設定したときのグラフであり、この場合を条件 C とする。A のエリア数を 10 に設定し、C のエリア数を 4 に設定。エリア数を少なく変更すると、推定誤差の抑制に大きく影響することがわかる。

E_{ini} と E_{conv} の値の幅に関して、エリア数を変更した場合に対して標準偏差の幅を変更した場合のほうが比較的大きな影響がみられる。

第7章 まとめ

本稿では、総サンプリング数が一定であるという制約条件のもとで複数エリアからデータの収集を行う場合を想定し、単一エリアでワーカ数と推定誤差との関係を実験により示し、その性質を用いて全エリアの総推定誤差を最小化するサンプルワーカ数調整アルゴリズムを提案した。また、性能評価から以下のことを確認した。

- 各エリアの特性（ワーカの測定値の標準偏差）が異なる場合、同一サンプルワーカ数で比較すると標準偏差が小さいエリアほど推定精度が高くなる。
- 単一エリアでは、サンプルワーカ数の増加に伴い推定精度は向上する。
- 複数エリアの総推定誤差が最小になるようワーカ数を最適化すると、推定精度の低い標準偏差が大きなエリアに多くのワーカを配置するという結果が得られた。
- 総サンプルワーカ数の増加に伴い複数エリアでの推定精度は向上する。また、総サンプルワーカ数と他の条件に関して同一で、標準偏差とエリア数をそれぞれ変化させたものを比較すると、標準偏差の幅が大きいものほど推定誤差は大きく、エリア数は少ないほど推定誤差が小さくなるという結果が得られた。

今後はサンプリングを想定した効率的な攻撃ワーカの配置方法を提案し、さらにユーザーにインセンティブを支払うモデルを考慮したサンプリングワーカの実選による防御法の確立を目指す。

謝辞

本研究を行うに当たり，ご指導を頂いた上山教授に感謝します．また日常，有益な議論をして頂いた研究室の皆様にも感謝します．

参考文献

- [1] Q. Li, et al., Conflicts to Harmony: A Framework for Resolving Conflicts in Heterogeneous Data by Truth Discovery, *IEEE Trans. Know. Data Eng.*, 28 (8), Aug. 2016
- [2] Z. Huang, M. Pan, and Y. Gong, Robust Truth Discovery Against Data Poisoning in Mobile Crowdsensing, *IEEE GLOBECOM* 2019
- [3] K. Quintal, E. Kara, M. Simsek, B. Kantarci, and H. Viktor, Sensory Data-driven Modeling of Adversaries in Mobile Crowd sensing Platforms, *IEEE GLOBECOM* 2019
- [4] C. Miao, Q. Li, L. Su, M. Huai, W. Jiang, and J. Gao, Attack under Disguise: An Intelligent Data Poisoning Attack Mechanism in Crowdsourcing, *WWW* 2018
- [5] C. Miao, Q. Li, H. Xiao, W. Jiang, M. Huai, and L. Su, Towards Data Poisoning Attacks in Crowd Sensing Systems, *ACM Mobihoc* 2018
- [6] L. Varshney, Privacy and Reliability in Crowdsourcing Service Delivery, *SRII* 2012
- [7] R. Fujimoto and N. Kamiyama, Poisoning Attacks in Crowdsensing Over Multiple Areas, *IEEE GLOBECOM* 2022