

# 多地域Crowdsensingにおける ワーカ最適サンプリング

## 1. 研究背景

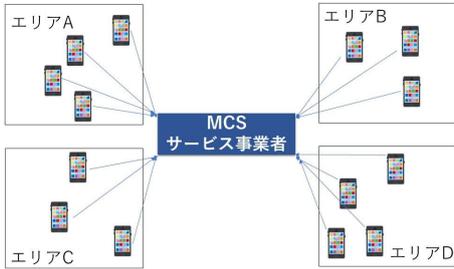
- MCS(モバイルクラウドセンシング)
  - モバイル機器をIoTデバイスとして活用
  - 今日のモバイル機器は様々なセンシング機能が搭載
  - 多くのユーザが取得したデータを収集することが出来る



- MCSのメリット
  - インフラの新規構築が不要であり低コスト
  - 従来のIoTデバイスより高機能
  - 普及率が高く膨大なデータを収集することができる
- MCSのデメリット
  - センサーの不具合やヒューマンエラーによった誤ったデータの発生

意図的に誤差の大きなデータを送信することで推定値を歪ませるデータポイズニング攻撃の問題が指摘

- データプライバシーの漏洩問題
  - データのアップロード時にバッテリー消耗や個人情報の漏洩などのリスクが発生
  - データを提供してもらうための動機付けが必要
  - 例: インセンティブ
- 複数エリアを対象としたCrowdsensing
  - 複数の地点からセンシングデータを集め、エリアごとに値を推定するサービス
  - 例: 気象情報



- 単一エリアで適用可能なアルゴリズム
  - CRH法
  - 誤差を抑制するように推定値を設定

## 2. 研究の目的

- 複数地域を対象とした防御法は未検討
- サービス事業者のインセンティブ予算の制約により、データ収集数は限定される

複数地域を想定し、収集数が固定である条件のもとでも高い推定精度を実現できるようなアルゴリズムの提案

## 3. CRH法

- CRH(Conflict Resolution on Heterogeneous data)
  - 目的: 複数のソースから得られた値から真実を推定する
  - アルゴリズム

- (i) 各ユーザ  $k$  の信頼性 (重み)  $w_k$  を 1 に初期化
- (ii) 式 (1) で、各ユーザ  $k$  の報告値  $v_k$  と  $w_k$  から、推定値  $\bar{v}$  を計算

$$\bar{v} = \frac{\sum_{k \in N \cup A} v_k w_k}{\sum_{k \in N \cup A} w_k} \quad (1)$$

- (iii) 式 (2) でユーザごとの信頼性  $w_k$  を更新

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

- (iv)  $\bar{v}$  及び  $w_k$  が収束するまで (ii)(iii) を反復

N: 正常ユーザの集合      A: 攻撃者の集合

## 4. 提案方式

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

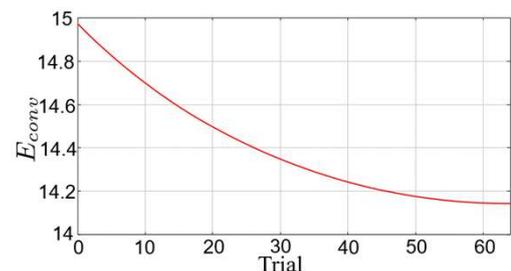
- 最適化問題
  - 目的関数
  - エリア  $i$  の推定値を  $v_i$ 、真の値を  $p_i$  とすると、各エリアの誤差は  $|v_i - p_i|$  と表される ( $K$ : エリア数)

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

- アルゴリズムの概要
  1. 各エリアのサンプルワーカ数の初期値を  $u_i = N/K$  に初期化し、このときの総誤差  $E_{ini}$  を算出
  2. 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し、各エリアのサンプルワーカ数に対する平均推定誤差  $e_{i,u_i}$  の近似解を得る (DBIに格納)
  3. 各エリア  $i$  のサンプル人数をインクリメント (デクリメント) し、推定誤差の減少量  $e_{dec}$  (増加量  $e_{inc}$ ) を算出
  4. 減少量が最大であるエリアのサンプル人数をインクリメント、増加量が最小であるエリアのサンプル人数をデクリメント
  5. 総誤差の変化量  $|E_{post} - E_{pre}|$  が閾値  $\eta$  を下回るまでこれを反復し、このときの総誤差  $E_{conv}$  を算出

## 5. 評価結果

- 収集数調整回数に伴う総誤差の推移
- 例: 各エリアのユーザ測定値の標準偏差が異なる場合



- 提案方式を適用すると、調整を行う毎に総誤差は減少
- データポイズニング攻撃が行われた際も有効であることを明らかにした