攻撃者が存在する場合の 多地域Crowdsensingのワーカ最適サンプリング法の性能評価

Performance Evaluation of Optimum Worker Sampling in Crowdsensing with Multiple Areas under Attacks

松浦 千紘[1]　上山 憲昭[2]
Chihiro Matsuura　Noriaki Kamiyama
立命館大学 情報理工学研究科[1]
Graduate School of Information Science and Engineering, Ritsumeikan University
立命館大学 情報理工学部[2]
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

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，様々なワーカ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．ワーカ推定誤差を最小化するよう各ワーカの測定値を重みづけした重みづけ平均で推定する CRH（Conflict Resolution on Heterogeneous data）法がある [1]．また，この CRH 法を活用して，悪意のあるワーカ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]．これらを用いて，筆者らは複数エリアごとに複数ワーカから測定値を推定する MCS において，攻撃ワーカが推定誤差を最大化するよう各エリアの配置攻撃者数を最適化する方式を提案した [3]．しかし [1][2][3] では各エリアに存在する全ワーカからデータを収集するが，ワーカ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，実際には一定の確率でサンプルしたワーカからのみデータを収集することが予想される．そこで筆者らは，複数エリア MCS において，全エリアの誤差総和の最小化を目的とした各エリアの最適サンプル数設定法を提案した [4]．本稿では，攻撃者が DPA 法により攻撃を行った場合において，提案方式を適用することでどの程度，推定精度の劣化を回避できるかを評価する．

2. CRH 法

CRH 法は，複数の測定値から真の値を推測することを目的としたアルゴリズムである [1]．推定値と測定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各ワーカの信頼性を設定し，信頼性を重みとした測定値の加重平均を推定値として用いる．ワーカの k の重みを w_k，正常ワーカの集合を N，攻撃ワーカの集合を A とすると，各ワーカの重み w_k と推定値 $\tilde{v}$ は以下の式で導出される．

$$w_k = -\log \frac{(v_k - \tilde{v})^2}{\sum_{k \in N \cup A} (v_k - \tilde{v})^2} \tag{1}$$

$$\tilde{v} = \frac{\sum_{k \in N \cup A} v_k w_k}{\sum_{k \in N \cup A} w_k} \tag{2}$$

3. 提案方式

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．ただし総エリア数を K とし，各エリアの推定値を CRH 法を利用して算出する．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 (3) 式で与える． また制約条件を (4) 式で与える．

$$\min E(u_1, u_2, \cdots, u_K) = \sum_{I=1}^{K} (v_i - p_i)^2 \tag{3}$$

$$\sum_{i=1}^{K} u_i = N \tag{4}$$

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. 各エリアのサンプルワーカ数の初期値を $u_i = N/K$ 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
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 総誤差の変化量 $|E_{post} - E_{pre}|$ が閾値 η を下回るまで，step 3 〜 step 7 を反復
9. step 8 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

4. 性能評価

各エリアの測定値の平均 μ_i を 50 ，各エリアの標準偏差 σ_i を最小 2，最大 11 の 1.0 刻みで設定し，エリア数を 10 個，総サンプルワーカ数を 400 人とする．攻撃ワーカの測定値の初期値を 50 とし，各エリアの攻撃ワーカの割合を 0.05 とする．[2] より，DPA 法適用時の攻撃ワーカ割合は 0.2 以下であるから，サンプリング時の各エリアの攻撃ワーカ割合は最大 0.2 と仮定する．また，t_0 を初期測定時刻とし，提案方式を適用し調整を行った後の測定時刻を t_1 とする．時刻 t_0 に各エリアのサンプルワーカ数 u_i に対して，$0.2u_i$ 以下の数の攻撃ワーカがサンプルされると仮定する．

図 1 は，各測定時刻における総誤差を示している．$N = 400$ より S_0 のとき $u_i = 40$ であるが，提案方式を適用すると (t_1)，各エリアのサンプルワーカ数は，標準偏差が小さいエリアから順に，17，23，29，34，38，44，47，52，56，60 となった．標準偏差が小さいエリアは推定誤差が小さく，また正常ユーザの数が多いほど誤差は小さくなる．一方でサンプルワーカ数の増加に伴い推定誤差は減少するため，誤差の大きなエリアに多くのサンプルワーカが割り当てられる．サービス事業者は収集データの区別ができない条件のもとでサンプリングを行っているが，一定の割合で攻撃データが混在している状態においても本提案方式は有効であることがわかる．

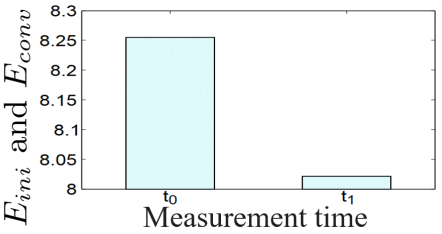

図 1: 各測定時刻における総誤差

謝辞 本研究成果は，JSPS 科研費 21H03437 の援助を受けたものである．ここに記して謝意を表す．

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] R. Fujimoto and N. Kamiyama, Poisoning Attacks in Crowdsensing Over Multiple Areas, IEEE GLOBECOM 2022.
[4] 松浦 千紘，上山 憲昭, 多地域 Crowdsensing におけるワーカ最適サンプリング, 信学会 NS 研究会, NS2022-218, 2023 年 3 月