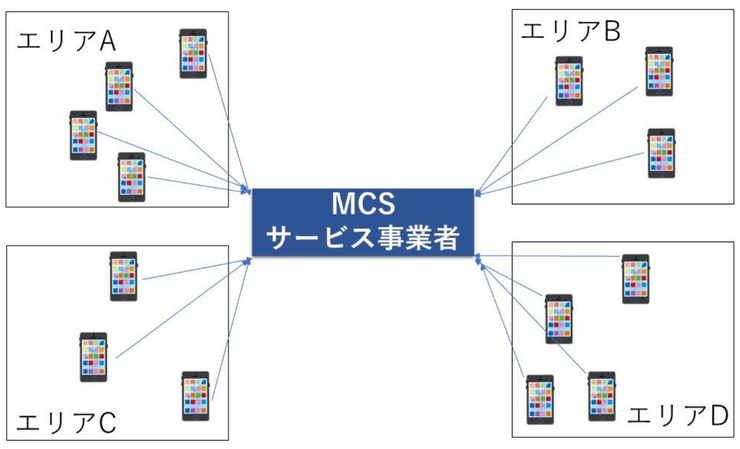
Crowdsensing における Data Poisoning 攻撃の秘密分散を用いた防御法

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可能



■ 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

■ DPA（Data Poisoning Attack）
- ➢ 推定誤差を大きくするように攻撃者の値を設定するアルゴリズム

■ 既存研究：複数エリアを対象としたCrowdsensing
- ➢ 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の提案

2. 研究の目的

■ 上記の既存研究では総誤差の減少を確認したものの，DPA 攻撃による影響は大きく，大幅な削減は実現できていない

■ 収集時のデータの漏洩問題について未検討である

秘密計算を導入することによりワーカのデータ保護し，悪意のあるワーカによるDPA攻撃の防御を行う

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 $\tilde{v}$ を計算

$$\tilde{v} = \frac{\sum_{k \in \boldsymbol{N} \vee \boldsymbol{A}} v_k w_k}{\sum_{k \in \boldsymbol{N} \vee \boldsymbol{A}} w_k} \tag{1}$$

（iii） 式 (2) でユーザごとの信頼性 w_k を更新

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

（iv） $\tilde{v}$ 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. DPA法

■ DPA（Data Poisoning Attack）
- ➢ 目的：CRH 法を利用して攻撃ユーザワーカの測定値を設定する
- ➢ アルゴリズム

（i） 各攻撃者 k の報告値 v_k の初期化

（ii） 正常ユーザのみで CRH 法を用いて推定値 $\tilde{v}$ を算出

（iii） 全ユーザを対象に CRH 法を用いて推定値 $\hat{v}$ を算出

（iv） 各攻撃者 K に対し，式 (3) で報告値 v_k を更新

$$v_k = v_k + 2 \times (\hat{v} - \tilde{v}) \times \frac{w_k}{\sum_{k \in \boldsymbol{N} \vee \boldsymbol{A}} w_k} \tag{3}$$

（v） v_k が収束するまで (ii)～(iv) を反復

5. 秘密計算

■ 秘密分散法（Secret Sharing Schemes）
- ➢ 秘密情報を分散して管理する方法
- ➢ 「シェア」と呼ばれるデータに分割するが，シェアはある定められた組み合わせが揃ったときのみ元の秘密情報が復元できるよう生成

■ 秘密分散法ベースの秘密計算
- ➢ k-out-of-n 閾値型秘密分散

メッセージ空間をM，シェア空間をS，分散アルゴリズムをShare，復元アルゴリズムをReconstとすると，以下のような関係を持つ
- Share(m) → s：秘密情報 $m \in M$ を入力として，n個のシェア $s = (s_1, \cdots, s_n) \in S^n$ を出力
- Reconst(s_I) → m’：$s_I = \{s_i\}_{i \in I}$ を入力として，メッセージ $m' \in M$ を出力

n 個のシェアのうち，任意の k(≤ n) 個のシェアを集めると元の秘密情報が復元でき，またどの k − 1 個のシェアを集めても元の秘密情報は一切漏れないという性質を持つ

6. 提案方式の概要

■ 攻撃者はすべての正常ワーカの通信路が傍受可能な環境を想定し，そのような状態でも攻撃者のシェアの復元を阻止する手法を提案

1. 正常ワーカの測定値に秘密分散法を適用し，複数のシェア（パケット）を作成
2. クラウドサーバが各正常ワーカに対し秘密裡に識別 ID セットを付与
3. 各パケットに自身に割り当てられた識別 ID セットの中の任意の ID を付与し，インターリーブ手法を用いてクラウドサーバへ送信
4. クラウドサーバは受信したパケットと，そのパケットを送信したワーカの対応を考慮して推定値計算を実行
5. 推定値計算のシェアを要求者の元へ送信し，要求者は閾値以上のシェアを受信した際に計算結果を復元

■ 通信経路においてシェア（パケット）のやり取りが行われるが，このとき各パケットを送信したワーカが誰であるか，すなわちパケットの組み合わせが不明であれば全てのデータが盗聴されても元データの復元は不可能

■ 今後，インターリーブの方式の遅延時間を評価