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

Defending against Data Poisoning Attacks in Crowdsensing with Secret Sharing

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]．サンプリングを用いた防御法などが研究されているが，DPA 攻撃による影響は大きく大幅な総誤差の削減は実現できていない．また，機密情報の漏洩などの問題からワーカはデータの共有時に懸念を持つ可能性がある．データの保護について堅牢なシステム構築がなされていない場合，ワーカはデータの提供に消極的になり品質の低下に繋がることから，個々のワーカのデータは十分に保護されるべきである．本稿では，秘密計算を導入することでワーカのデータを保護し，悪意のあるワーカによる DPA 攻撃を防御するシステムを提案する．

2. 秘密分散法ベースの秘密計算

秘密分散法 (Secret Sharing Schemes) は，秘密を分散して管理する方法として 1979 年に Shamir と Blakley によって提案された技術である．秘密分散法では，秘密情報を複数の「シェア」と呼ばれるデータに分割する．このシェアは，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に作られる．復元の条件を満たさないシェアのみが流出しても，元の秘密情報が漏れないことが保証される．最も単純であり，秘密計算において使われる一般的なものは k-out-of-n 閾値型秘密分散 ((k,n) 閾値法)[3] である．これは n 個のシェアのうち，任意の $k(\leq n)$ 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．

3. 提案方式の概要

本節では，提案方式の概要を説明する．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する．

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する
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である．それぞれのパケットにランダムに ID を付与し，インターリーブ手法を用いてパケットの発信タイミングをずらすことで，送信者との対応を困難にする．

4. インターリーブ手法の評価

攻撃者は正常データの値が未知である限り，DPA 法を用いて推定誤差の最大化に有効な測定値を設定することができない．従って，同一ワーカから送信されたパケットの組み合わせを知られないことが重要である．そこで複数の異なるワーカが送信したパケットが通信路上で混ざるよう，ランダムにパケット送信を行うインターリーブ手法を提案する．どのような条件下であればランダム性の高い送信方法を実現できるのか，パケットの送信間隔に焦点を当てて実験を行った．総ワーカ数を 100 とし，各パケットの送信開始時刻は平均発生間隔 $1/\lambda$ の指数分布に従うものとする．図 1 は，1 つ目に送信されるパケットの各発生間隔における，他のワーカのパケットが混じらない連続送信の回数を示している．各ワーカから発信される 1 つ目のパケットの間隔が大きいほど，同一のワーカから発信されたパケットが隣り合うという傾向が確認された．また，1 つ目以降のパケットの発生間隔をそれぞれ $1/\lambda = 3, 10, 20$ とすると，発生間隔が小さいほど連続して送信されることがわかる．よって，パケットを送信する際に 1 つ目のパケットの送信間隔は小さく，以降のパケットの送信間隔は大きく送信することで，同一ワーカのデータが離れて送信される理想的な状況を実現できると言える．

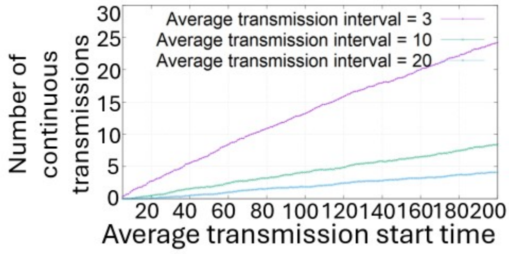

図 1: 1 つ目のパケットの各発生間隔における連続送信回数

次に，特定のワーカがパケットを送信する間に，他のワーカのパケットが割り込まない確率を導出する．平均発生回数を λ とした際に，任意の時間間隔 T において他のユーザがデータを送信しない確率は $e^{-\lambda T}$ であるから，特定のワーカが k 個のパケットを送信する間に他ワーカのパケットが割り込まない確率は，$P = (e^{-\lambda T})^{(k-1)(N-1)}$ と表される (総ワーカ数 N)．図 1 は，総ワーカ数を 100，$k = 3$ とした場合の，ある特定のワーカの各送信間隔における連続送信確率，すなわち他ワーカのパケットが割り込まない確率を示している．送信間隔の増加に伴い連続送信確率は急速に減少する．$k = 3$ 程度でも連続送信確率は非常に小さく，提案方式の有効性が確認できる．

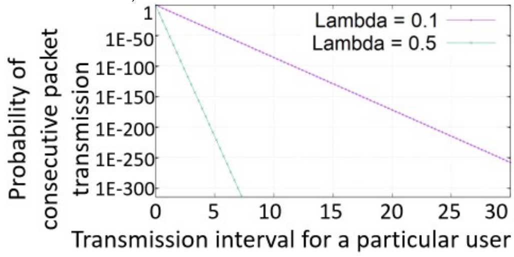

図 2: 特定のワーカの各送信間隔における連続送信確率

謝辞 本研究成果は，JSPS 科研費 23K28078 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] A. Shami, How to share a secret, Column. ACM, Vol. 22, No. 11, pp. 612-613, 1979.

Copyright © 2024 IEICE