

介護における音響 HAR と連合学習を用いた異常検知

竹本志恩

June 20, 2025

INIAD

背景と研究目的

- 高齢化社会における介護現場の負担増大
- HAR に着目: 介護者の負担軽減
- センサー／音響データのプライバシー懸念
- 目的: 異常イベントをリアルタイム検知＋通知

本研究の独自性

- 複数の異常イベントを同時／複合的に検知
- マルチラベル分類で音響イベントを解釈
 - | -例 1: 咳と苦痛の音が同時に聞こえる > 重篤な状態
 - | -例 2: 転倒に似た音を, 他のイベントを基に判断
- 深い状況把握と迅速対応支援を実現

- 非接触モニタリング＋視覚プライバシー保護
- 環境騒音によるマスキング
- 高静音性活動の検知が困難
- 音の多様性／同時発生の問題
 - ＞ 頑健なモデルが必要

連合学習 (FL) の基礎と HAR への適用

- 分散学習：生データ非共有でモデル協調学習
- プライバシー保護、パーソナル化、通信効率
- 介護現場に適した技術

FL-HARの主要課題

主要課題①：データ関連

- 極端なデータ不均衡（稀イベント、多ラベル共起）
 - └ 複数異常の組み合わせはほぼない
- Non-IID 分布
 - └ 各利用者の音響特性や行動の差
- ラベルの関係を捉えたモデリング
- マルチラベル異常データセットの不足

主要課題②：モデル・通信・プライバシー

- モデル複雑化 <—> 通信オーバーヘッド
- リアルタイム通知の遅延リスク
- 稀な複合イベントの機密性への影響

主要課題③：パーソナライズ化・継続学習

- 個人差対応のパーソナライズド FL
- コールドスタート：未知の音響組み合わせ
- 音響環境変化への適応

課題解決の戦略

対策①：データ不均衡・Non-IID 対策

- 合成データ生成 (GAN, SMOTE)
- 少数クラスを強調: Time-Balanced Focal Loss など特殊損失
- パーソナライズド FL: FedProx, SCAFFOLD
- モデル統合の効率化: クラスタリング FL / ドメイン適応

対策②：プライバシー強化

- オンデバイス特徴抽出によるデータ最小化
- ノイズ付与: 差分プライバシー (DP)
- 暗号化集約: セキュアアグリゲーション (SA) ／同型暗号 (HE)
- 精度とオーバーヘッドのバランス

対策③：モデル・リソース効率化

- モデル軽量化: モデル圧縮/量子化/枝刈り
- 計算の分割: Federated Split Learning (FSL)
- 通信量削減: 勾配圧縮・選択的更新

- 標準化データセットの整備
- FL 対応マルチラベル損失／新アーキテクチャ開発
|— マルチラベル FL など参考
- 連合継続学習
- 因果推論の検討

補足資料

データ不均衡・Non-IID への対応：SMOTE

- 概要：Synthetic Minority Over-sampling Technique の略
- 目的：少数クラスのデータ不足に起因する不均衡を緩和
- 動作原理：既存の少数サンプル間の特徴空間で補間することで、合成サンプルを生成。音響データの場合、MFCC などの抽出された音響特徴量に適用
- 利点と課題：
 - 実装が比較的容易で、多くのライブラリで利用可能
 - 単純な適用では過学習の可能性
 - 音響的に意味のある合成サンプルを生成できない、時間的連続性が破壊される可能性も
 - 希少イベント固有の音響特性を保持することが重要

データ不均衡・Non-IID への対応：Time-Balanced Focal Loss

- 概要：持続時間のばらつきによるデータ不均衡を考えた損失関数
- 目的：イベントの発生頻度だけでなく、持続時間も考慮
- 動作原理：
 - 標準的な Focal Loss をクラスごとの重み w_c で拡張
 - w_c は、データ量（音源/クリップ数）とイベント持続時間（フレームの比率 r_c ）を考慮
 - 希少で持続時間の短い音響イベントの学習が強化され、検出精度が向上

プライバシー強化技術：差分プライバシー (DP)

- 目的：個々のデータサンプルの寄与を曖昧にし、漏洩リスクを保証
- 動作原理：
 - モデル更新（勾配や重みなど）にノイズを付加
 - Federated Split Learning (FSL) では、中間活性化情報にガウスノイズ
- 課題：以下のトレードオフ
 - モデルの精度低下
 - 計算・通信オーバーヘッドの増加

リソース効率化技術：Federated Split Learning (FSL)

- 概要：モデルの計算負荷をクライアントとサーバーで分割
- 目的：エッジデバイスの計算能力、メモリ、通信帯域の制約を両立させながら、モデル訓練や推論を効率的に実行
- 動作原理：
 - モデルの層を分割点（‘cut layer’または‘split layer’）で分け、クライアント側でモデルの一部（例：特徴抽出層）を処理し、中間活性化情報をサーバーに送信
 - サーバー側で残りのモデル処理（例：分類層）、損失計算、およびバックプロパゲーションを実行
 - 例：クライアント側に LSTM 層、サーバー側に出力層（Dense+Softmax）を配置

マルチラベルFLフレームワーク：FMLL

- 動作原理：
 - マルチラベルデータセットをバイナリ関連性 (Binary Relevance) 戦略に基づき複数の二値データセットに分解
 - 各二値データセットでローカルモデル（例: REPTree）を訓練し、中央ノードでこれらのローカルモデルを集約してグローバルモデルを作成
- HAR 適用時の課題：
 - 現状、動物科学分野のデータセットで検証されており [33, 35]、HAR 異常データへの直接的な適用性は未検証
 - ベース分類器として REPTree を使用しており、表現力の限界が懸念

マルチラベル FL フレームワーク：FedMLP

- 概要：部分的なアノテーション（欠損ラベル）を持つマルチラベル FL に対応
- HAR 適用時の課題：
 - 医療データセットで検証されている
 - 疑似ラベリングの精度が全体の性能に影響を与える可能性

参考文献一覧

