連合学習における訓練データの一部共有による精度向上手法のテストベッドでの評価

岡田明日香　川上朋也　長谷川達人（福井大学）

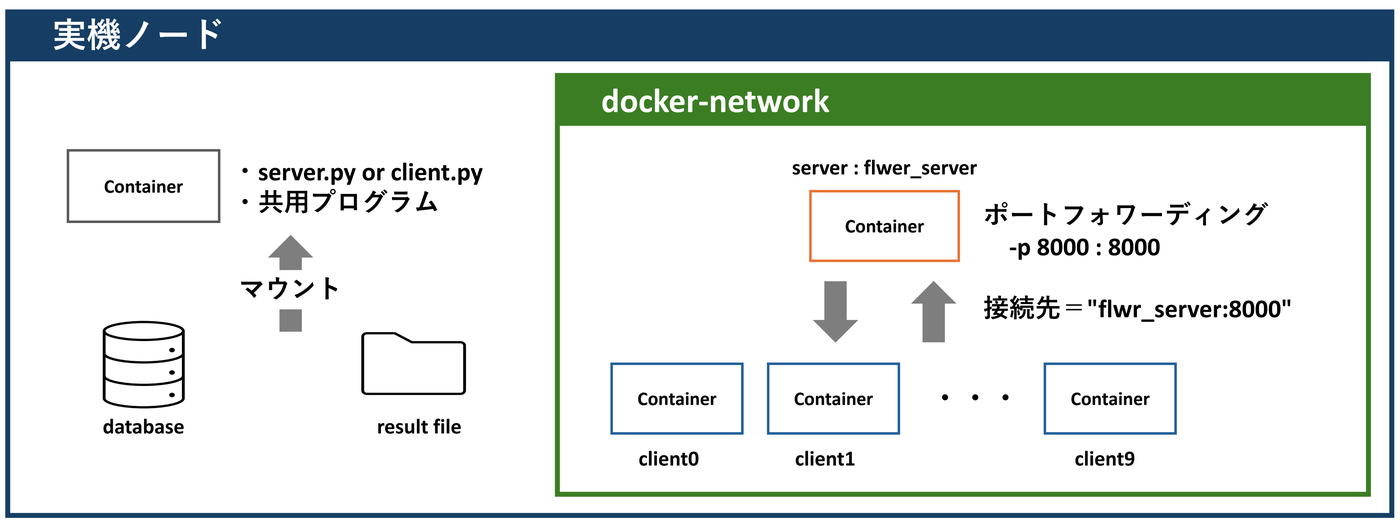
背景

- 特にデータのプライバシーの観点で，**連合学習による分散型検知**が注目
- 検知の精度を向上するため，我々は先行研究[1]において**「訓練データの一部をクライアント間で共有する」**という新しい考えを提案
- ネットワーク侵入検知システム（NIDS）を例として，シミュレーションで評価していた先行研究を**DockerおよびStarBED上で評価**

検証環境

- テストベッド：StarBED
- 実機ノード：1台
- Dockerコンテナ：11台
  - ・サーバ　　：1台
  - ・クライアント　：10台
- docker composeにより一括管理
- データセットや結果格納先は外部からマウント

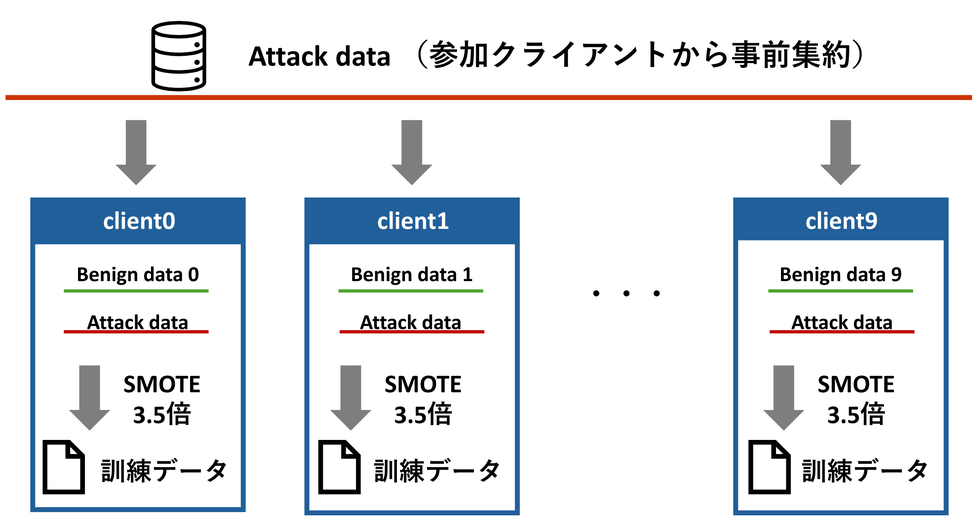
※単一実機上で論理的に分離された分散環境を構築



提案手法

FLにおける**攻撃データのクライアント間共有の許可**

＋**正常・攻撃両データのSMOTE[2]アップサンプリング**



実験設定

- 提案手法FL

  攻撃データ共有

  SMOTE：3.5
- 比較手法FL

  各クライアント内で

  攻撃データを10倍に複製
- 中央集約型学習

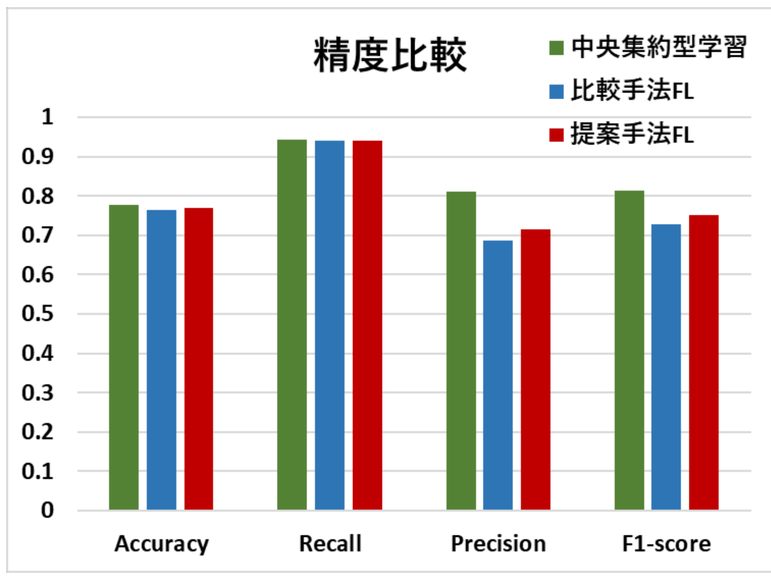
  連合学習なし

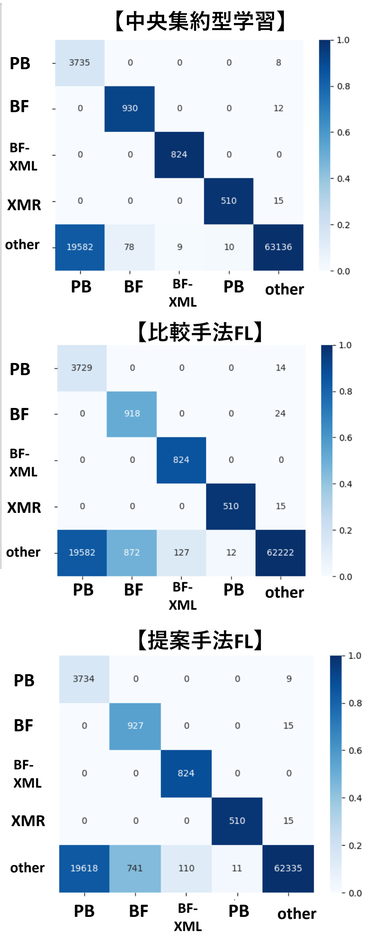
  ローカル環境で実施

  攻撃データの10倍複製

連合学習	
FLフレームワーク	Flower[3]
集約アルゴリズム	Federatede Averaging
クライアント数	10
連合学習ラウンド数	60
クライアントモデル	
機械学習ライブラリ	TensorFlow
モデル	Multi-layer-Perceptoron
ニューロン数	[128, 64, 5]
活性化関数	隠れ層 : relu, 出力層 : softmax
バッチサイズ	32
最適化アルゴリズム	Adam
学習率	0.00001
早期終了	patience : 10, min_delta : 0.001
データセット	
データセット	HIKARI-2021[4]
ラベル	Traffic_category
使用特徴量数	81（数値型のみ）

評価





※本実験ではPrecision視点で色付け

- RecallはFLと中央集約型学習で同程度
- Precision, F1-scoreが約3%向上
- 正常データ（other）をBruteforceと誤検知する件数が減少
- Probingは正常通信と特徴が似ており判別が難しい
- 中央集約型学習では正常データの誤検知率がさらに低い
- 攻撃データ共有やSMOTEにより**データのバリエーション増加**
  - ▶ モデルの精度向上

今後の展望

- 複数ノードを用いて分散実証実験の実施
- 特定クライアントの処理が遅いケースの実験
- クライアント数変動の影響調査

本研究は総務省FORWARD（受付番号JPMI250520001）および福井大学学長裁量経費による成果である．

参考文献
[1] A. Okada *et al.*: An Accuracy Improvement Method by Sharing Attack Data in Federated Learning-Based NIDS, *Proc. ICMU 2025*, pp. 138–143 (2025).
[2] N. V. Chawla *et al.*: SMOTE: Synthetic Minority Over Sampling Technique, *Journal of Artificial Intelligence Research*, Vol. 16, pp. 321–357 (2002).
[3] D. J. Beuteletal: Flower: A friendly Federated Learning Research Framework, *arXiv:2007.14390*, pp. 1–22 (2020).
[4] A. Ferriyan *et al.*: Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic, *Applied Sciences*, Vol. 11, No. 7868, pp. 1–17 (2021).