FL Simulation Results

File: test1.3_

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 5

Neural Network: MyNN

Training Rounds: 5

Poisoned Rounds (R): 5

Distribution Strategy: first

Data Poisoning Attack Parameters

Poisoning Operation: Label Flip

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using label_flip with 15.0% (0.15) intensity on 30.0% (0.30) of data for 5 rounds with 5 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9353

Poisoned Accuracy: 0.7522

Poisoned + DP Protection Accuracy: 0.7630

Drop (Clean - Poisoned): 0.1831

Drop (Clean - Init): -0.0092

Drop (Poisoned - Init): -0.1923

Drop (Poisoned DP - Init): -0.1815

DP Protection Method: fedavg

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9366

Clean Recall: 0.9353

Clean F1 Score: 0.9352

Poisoned Precision: 0.7772

Poisoned Recall: 0.7779

Poisoned F1 Score: 0.7744

DP Protection Precision: 0.7776

DP Protection Recall: 0.7898

DP Protection F1 Score: 0.7802

Summary

FL Simulation Complete
Task: 55ded522-c84d-4723-adbc-2d323bee71b8
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9353
Poisoned Accuracy: 0.7522
Data Poison Protection Accuracy: 0.7630
Drop (Clean - Poisoned): 0.1831
Drop (Clean - Init): -0.0092
Drop (Poisoned - Init): -0.1923
Drop (Poisoned_DP - Init): -0.1815
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9366
Clean Recall: 0.9353
Clean F1 Score: 0.9352
Poisoned Precision: 0.7772
Poisoned Recall: 0.7779
Poisoned F1 Score: 0.7744
DP Protection Precision: 0.7776
DP Protection Recall: 0.7898
DP Protection F1 Score: 0.7802