FL Simulation Results

File: test_LabelFlip

Federated Learning Configuration

Total Clients (N): 5

Malicious Clients (M): 1

Neural Network: Test1.1_

Training Rounds: 2

Poisoned Rounds (R): N/A

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 0 rounds with 1 malicious clients.

Simulation Results

Init Accuracy: 0.7334

Clean Accuracy: 0.8442

Clean + DP Protection Accuracy: 0.8438

Poisoned Accuracy: 0.6288

Poisoned + DP Protection Accuracy: 0.6058

Drop (Clean - Poisoned): 0.2154

Drop (Clean - Init): 0.1108

Drop (Clean DP - Init): 0.1104

Drop (Poisoned - Init): -0.1046

Drop (Poisoned DP - Init): -0.1276

DP Protection Method: trimmed_mean

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8457
Clean Recall: 0.8442
Clean F1 Score: 0.8431

Clean DP Precision: 0.8485
Clean DP Recall: 0.8438
Clean DP F1 Score: 0.8447

Poisoned Precision: 0.6750
Poisoned Recall: 0.6432
Poisoned F1 Score: 0.6453

DP Protection Precision: 0.6797
DP Protection Recall: 0.6180
DP Protection F1 Score: 0.6292

Summary

```
FL Simulation Complete
Task: 059ef46e-520b-4eda-955c-ab0b0da60bd5
GPU: GPU 1
Init Accuracy: 0.7334
Clean Accuracy: 0.8442
Clean DP Accuracy: 0.8438
Poisoned Accuracy: 0.6288
Data Poison Protection Accuracy: 0.6058
Drop (Clean - Poisoned): 0.2154
Drop (Clean - Init): 0.1108
Drop (Clean DP - Init): 0.1104
Drop (Poisoned - Init): -0.1046
Drop (Poisoned_DP - Init): -0.1276
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8457
Clean Recall: 0.8442
Clean F1 Score: 0.8431
Clean DP Precision: 0.8485
Clean DP Recall: 0.8438
Clean DP F1 Score: 0.8447
Poisoned Precision: 0.6750
Poisoned Recall: 0.6432
Poisoned F1 Score: 0.6453
DP Protection Precision: 0.6797
DP Protection Recall: 0.6180
DP Protection F1 Score: 0.6292
```