FL Simulation Results

File: test1.1__

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 1

Neural Network: Test1.1_

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 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9262

Poisoned Accuracy: 0.6767

Poisoned + DP Protection Accuracy: 0.6119

Drop (Clean - Poisoned): 0.2495

Drop (Clean - Init): -0.0183

Drop (Poisoned - Init): -0.2678

Drop (Poisoned DP - Init): -0.3326

DP Protection Method: median

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9280

Clean Recall: 0.9262

Clean F1 Score: 0.9260

Poisoned Precision: 0.7565

Poisoned Recall: 0.6882

Poisoned F1 Score: 0.6820

DP Protection Precision: 0.7597

DP Protection Recall: 0.6162

DP Protection F1 Score: 0.6231

Summary

```
FL Simulation Complete
Task: 73c667df-682b-4ab3-8dd6-c4b1ec26a8e9
GPU: GPU 1
Init Accuracy: 0.9445
Clean Accuracy: 0.9262
Poisoned Accuracy: 0.6767
Data Poison Protection Accuracy: 0.6119
Drop (Clean - Poisoned): 0.2495
Drop (Clean - Init): -0.0183
Drop (Poisoned - Init): -0.2678
Drop (Poisoned_DP - Init): -0.3326
Data Poison Protection Method: median
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9280
Clean Recall: 0.9262
Clean F1 Score: 0.9260
Poisoned Precision: 0.7565
Poisoned Recall: 0.6882
Poisoned F1 Score: 0.6820
DP Protection Precision: 0.7597
DP Protection Recall: 0.6162
DP Protection F1 Score: 0.6231
```