FL Simulation Results

File: test1.1

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 1

Neural Network: MyNN

Training Rounds: 5

Poisoned Rounds (R): 3

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 3 rounds with 1 malicious clients.

Simulation Results

Init Accuracy: 0.8807

Clean Accuracy: 0.5285

Poisoned Accuracy: 0.1563

Poisoned + DP Protection Accuracy: 0.1701

Drop (Clean - Poisoned): 0.3722

Drop (Clean - Init): -0.3522

Drop (Poisoned - Init): -0.7244

Drop (Poisoned DP - Init): -0.7106

DP Protection Method: fedavg

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.7509

Clean Recall: 0.5285

Clean F1 Score: 0.5148

Poisoned Precision: 0.4800

Poisoned Recall: 0.1204

Poisoned F1 Score: 0.0627

DP Protection Precision: 0.5054

DP Protection Recall: 0.1349

DP Protection F1 Score: 0.0865

Summary

FL Simulation Complete
Task: 5a63243f-c53c-4838-81df-20e4c9129d79
GPU: GPU 2
Init Accuracy: 0.8807
Clean Accuracy: 0.5285
Poisoned Accuracy: 0.1563
Data Poison Protection Accuracy: 0.1701
Drop (Clean - Poisoned): 0.3722
Drop (Clean - Init): -0.3522
Drop (Poisoned - Init): -0.7244
Drop (Poisoned_DP - Init): -0.7106
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.7509
Clean Recall: 0.5285
Clean F1 Score: 0.5148
Poisoned Precision: 0.4800
Poisoned Recall: 0.1204
Poisoned F1 Score: 0.0627
DP Protection Precision: 0.5054
DP Protection Recall: 0.1349
DP Protection F1 Score: 0.0865