FL Simulation Results

File: test1.2

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 3

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 3 malicious clients.

Simulation Results

Init Accuracy: 0.8807

Clean Accuracy: 0.6315

Poisoned Accuracy: 0.2230

Poisoned + DP Protection Accuracy: 0.2234

Drop (Clean - Poisoned): 0.4085

Drop (Clean - Init): -0.2492

Drop (Poisoned - Init): -0.6577

Drop (Poisoned DP - Init): -0.6573

DP Protection Method: fedavg

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.7355

Clean Recall: 0.6315

Clean F1 Score: 0.6176

Poisoned Precision: 0.8072

Poisoned Recall: 0.1919

Poisoned F1 Score: 0.1786

DP Protection Precision: 0.6938

DP Protection Recall: 0.1923

DP Protection F1 Score: 0.1810

Summary

FL Simulation Complete
Task: aceeb6f0-5eae-4424-a28a-397ceaefabdd
GPU: GPU 0
Init Accuracy: 0.8807
Clean Accuracy: 0.6315
Poisoned Accuracy: 0.2230
Data Poison Protection Accuracy: 0.2234
Drop (Clean - Poisoned): 0.4085
Drop (Clean - Init): -0.2492
Drop (Poisoned - Init): -0.6577
Drop (Poisoned_DP - Init): -0.6573
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.7355
Clean Recall: 0.6315
Clean F1 Score: 0.6176
Poisoned Precision: 0.8072
Poisoned Recall: 0.1919
Poisoned F1 Score: 0.1786
DP Protection Precision: 0.6938
DP Protection Recall: 0.1923
DP Protection F1 Score: 0.1810