FL Simulation Results

File: test1.1_

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 5

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 5 malicious clients.

Simulation Results

Init Accuracy: 0.8807

Clean Accuracy: 0.5074

Poisoned Accuracy: 0.2160

Poisoned + DP Protection Accuracy: 0.2145

Drop (Clean - Poisoned): 0.2914

Drop (Clean - Init): -0.3733

Drop (Poisoned - Init): -0.6647

Drop (Poisoned DP - Init): -0.6662

DP Protection Method: fedavg

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.7240

Clean Recall: 0.5074

Clean F1 Score: 0.4865

Poisoned Precision: 0.7000

Poisoned Recall: 0.1832

Poisoned F1 Score: 0.1378

DP Protection Precision: 0.5615

DP Protection Recall: 0.1818

DP Protection F1 Score: 0.1381

Summary

FL Simulation Complete

Task: 983668c1-f3f4-4e24-89cd-d40bd36f965d

GPU: GPU 1

Init Accuracy: 0.8807

Clean Accuracy: 0.5074

Poisoned Accuracy: 0.2160

Data Poison Protection Accuracy: 0.2145

Drop (Clean - Poisoned): 0.2914

Drop (Clean - Init): -0.3733

Drop (Poisoned - Init): -0.6647

Drop (Poisoned_DP - Init): -0.6662

Data Poison Protection Method: fedavg

--- Confusion Matrix Metrics (Weighted Avg) ---

Clean Precision: 0.7240

Clean Recall: 0.5074

Clean F1 Score: 0.4865

Poisoned Precision: 0.7000

Poisoned Recall: 0.1832

Poisoned F1 Score: 0.1378

DP Protection Precision: 0.5615

DP Protection Recall: 0.1818

DP Protection F1 Score: 0.1381