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: 0.9144

Poisoned Accuracy: 0.6177

Poisoned + DP Protection Accuracy: 0.5364

Drop (Clean - Poisoned): 0.2967

Drop (Clean - Init): -0.0301

Drop (Poisoned - Init): -0.3268

Drop (Poisoned DP - Init): -0.4081

DP Protection Method: trimmed_mean

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9207

Clean Recall: 0.9144

Clean F1 Score: 0.9149

Poisoned Precision: 0.7652

Poisoned Recall: 0.6274

Poisoned F1 Score: 0.6600

DP Protection Precision: 0.7710

DP Protection Recall: 0.5380

DP Protection F1 Score: 0.5647

Summary

FL Simulation Complete
Task: 74537c35-8aee-47b0-8437-47d0df6b8a70
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9144
Poisoned Accuracy: 0.6177
Data Poison Protection Accuracy: 0.5364
Drop (Clean - Poisoned): 0.2967
Drop (Clean - Init): -0.0301
Drop (Poisoned - Init): -0.3268
Drop (Poisoned_DP - Init): -0.4081
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9207
Clean Recall: 0.9144
Clean F1 Score: 0.9149
Poisoned Precision: 0.7652
Poisoned Recall: 0.6274
Poisoned F1 Score: 0.6600
DP Protection Precision: 0.7710
DP Protection Recall: 0.5380
DP Protection F1 Score: 0.5647