FL Simulation Results

File: test2.3

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: 0.7335

Clean Accuracy: 0.8609

Poisoned Accuracy: 0.6847

Poisoned + DP Protection Accuracy: 0.6788

Drop (Clean - Poisoned): 0.1762

Drop (Clean - Init): 0.1274

Drop (Poisoned - Init): -0.0488

Drop (Poisoned DP - Init): -0.0547

DP Protection Method: trimmed_mean

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8626

Clean Recall: 0.8609

Clean F1 Score: 0.8591

Poisoned Precision: 0.6848

Poisoned Recall: 0.7061

Poisoned F1 Score: 0.6931

DP Protection Precision: 0.6825

DP Protection Recall: 0.7000

DP Protection F1 Score: 0.6870

Summary

FL Simulation Complete
Task: ea5cfe23-1ed8-4d7c-a40f-05410e1d441d
GPU: GPU 0
Init Accuracy: 0.7335
Clean Accuracy: 0.8609
Poisoned Accuracy: 0.6847
Data Poison Protection Accuracy: 0.6788
Drop (Clean - Poisoned): 0.1762
Drop (Clean - Init): 0.1274
Drop (Poisoned - Init): -0.0488
Drop (Poisoned_DP - Init): -0.0547
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8626
Clean Recall: 0.8609
Clean F1 Score: 0.8591
Poisoned Precision: 0.6848
Poisoned Recall: 0.7061
Poisoned F1 Score: 0.6931
DP Protection Precision: 0.6825
DP Protection Recall: 0.7000
DP Protection F1 Score: 0.6870