FL Simulation Results

File: test2.4

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: 0.7334

Clean Accuracy: 0.8654

Poisoned Accuracy: 0.6790

Poisoned + DP Protection Accuracy: 0.6770

Drop (Clean - Poisoned): 0.1864

Drop (Clean - Init): 0.1320

Drop (Poisoned - Init): -0.0544

Drop (Poisoned DP - Init): -0.0564

DP Protection Method: trimmed_mean_krum

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8661

Clean Recall: 0.8654

Clean F1 Score: 0.8645

Poisoned Precision: 0.6896

Poisoned Recall: 0.7008

Poisoned F1 Score: 0.6918

DP Protection Precision: 0.6906

DP Protection Recall: 0.6978

DP Protection F1 Score: 0.6922

Summary

FL Simulation Complete
Task: 3764ff39-896f-4fb8-88a2-4f11478513f0
GPU: GPU 0
Init Accuracy: 0.7334
Clean Accuracy: 0.8654
Poisoned Accuracy: 0.6790
Data Poison Protection Accuracy: 0.6770
Drop (Clean - Poisoned): 0.1864
Drop (Clean - Init): 0.1320
Drop (Poisoned - Init): -0.0544
Drop (Poisoned_DP - Init): -0.0564
Data Poison Protection Method: trimmed_mean_krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8661
Clean Recall: 0.8654
Clean F1 Score: 0.8645
Poisoned Precision: 0.6896
Poisoned Recall: 0.7008
Poisoned F1 Score: 0.6918
DP Protection Precision: 0.6906
DP Protection Recall: 0.6978
DP Protection F1 Score: 0.6922