FL Simulation Results

File: test1.3

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: 0.5692

Poisoned Accuracy: 0.2644

Poisoned + DP Protection Accuracy: 0.2533

Drop (Clean - Poisoned): 0.3048

Drop (Clean - Init): -0.3115

Drop (Poisoned - Init): -0.6163

Drop (Poisoned DP - Init): -0.6274

DP Protection Method: fedavg

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.7335

Clean Recall: 0.5692

Clean F1 Score: 0.5629

Poisoned Precision: 0.7932

Poisoned Recall: 0.2357

Poisoned F1 Score: 0.2178

DP Protection Precision: 0.7981

DP Protection Recall: 0.2251

DP Protection F1 Score: 0.2251

Summary

FL Simulation Complete
Task: 7f1923e0-4bd3-4bb4-8c5d-72bd5c0c614c
GPU: GPU 0
Init Accuracy: 0.8807
Clean Accuracy: 0.5692
Poisoned Accuracy: 0.2644
Data Poison Protection Accuracy: 0.2533
Drop (Clean - Poisoned): 0.3048
Drop (Clean - Init): -0.3115
Drop (Poisoned - Init): -0.6163
Drop (Poisoned_DP - Init): -0.6274
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.7335
Clean Recall: 0.5692
Clean F1 Score: 0.5629
Poisoned Precision: 0.7932
Poisoned Recall: 0.2357
Poisoned F1 Score: 0.2178
DP Protection Precision: 0.7981
DP Protection Recall: 0.2251
DP Protection F1 Score: 0.2251