FL Simulation Results

File: test_LabelFlip_after_Modified_poison

Federated Learning Configuration

Total Clients (N): 5

Malicious Clients (M): 1

Neural Network: Test1.1_

Training Rounds: 3

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 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9466

Clean + DP Protection Accuracy: 0.0000

Poisoned Accuracy: 0.9378

Poisoned + DP Protection Accuracy: 0.0000

Drop (Clean - Poisoned): 0.0088

Drop (Clean - Init): 0.0021

Drop (Clean DP - Init): -0.9445

Drop (Poisoned - Init): -0.0067

Drop (Poisoned DP - Init): -0.9445

DP Protection Method: trimmed_mean

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9465
Clean Recall: 0.9466
Clean F1 Score: 0.9465

Clean DP Precision: 0.0000
Clean DP Recall: 0.0000
Clean DP F1 Score: 0.0000

Poisoned Precision: 0.9380
Poisoned Recall: 0.9378
Poisoned F1 Score: 0.9377

DP Protection Precision: 0.0000
DP Protection Recall: 0.0000
DP Protection F1 Score: 0.0000

Summary

FL Simulation Complete
Task: c57cdd45-5297-4a4e-a8a9-c7ddd2558e3d
GPU: GPU 1
Init Accuracy: 0.9445
Clean Accuracy: 0.9466
Clean DP Accuracy: 0.0000
Poisoned Accuracy: 0.9378
Data Poison Protection Accuracy: 0.0000
Drop (Clean - Poisoned): 0.0088
Drop (Clean - Init): 0.0021
Drop (Clean DP - Init): -0.9445
Drop (Poisoned - Init): -0.0067
Drop (Poisoned_DP - Init): -0.9445
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9465
Clean Recall: 0.9466
Clean F1 Score: 0.9465
Clean DP Precision: 0.0000
Clean DP Recall: 0.0000
Clean DP F1 Score: 0.0000
Poisoned Precision: 0.9380
Poisoned Recall: 0.9378
Poisoned F1 Score: 0.9377
DP Protection Precision: 0.0000
DP Protection Recall: 0.0000
DP Protection F1 Score: 0.0000