FL Simulation Results

File: test1.1_Trojan_Krum

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: backdoor_trojan

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using backdoor_trojan 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: 0.9441

Clean + DP Protection Accuracy: 0.9251

Poisoned Accuracy: 0.9244

Poisoned + DP Protection Accuracy: 0.9049

Drop (Clean - Poisoned): 0.0197

Drop (Clean - Init): -0.0004

Drop (Clean DP - Init): -0.0194

Drop (Poisoned - Init): -0.0201

Drop (Poisoned DP - Init): -0.0396

DP Protection Method: krum

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9444

Clean Recall: 0.9441

Clean F1 Score: 0.9438

Clean DP Precision: 0.9263

Clean DP Recall: 0.9251

Clean DP F1 Score: 0.9253

Poisoned Precision: 0.9249

Poisoned Recall: 0.9244

Poisoned F1 Score: 0.9235

DP Protection Precision: 0.9051

DP Protection Recall: 0.9049

DP Protection F1 Score: 0.9047

Summary

FL Simulation Complete
Task: d795e6e6-f95b-4e2e-8901-18e38af30c2c
GPU: GPU 1
Init Accuracy: 0.9445
Clean Accuracy: 0.9441
Clean DP Accuracy: 0.9251
Poisoned Accuracy: 0.9244
Data Poison Protection Accuracy: 0.9049
Drop (Clean - Poisoned): 0.0197
Drop (Clean - Init): -0.0004
Drop (Clean DP - Init): -0.0194
Drop (Poisoned - Init): -0.0201
Drop (Poisoned_DP - Init): -0.0396
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9444
Clean Recall: 0.9441
Clean F1 Score: 0.9438
Clean DP Precision: 0.9263
Clean DP Recall: 0.9251
Clean DP F1 Score: 0.9253
Poisoned Precision: 0.9249
Poisoned Recall: 0.9244
Poisoned F1 Score: 0.9235
DP Protection Precision: 0.9051
DP Protection Recall: 0.9049
DP Protection F1 Score: 0.9047