FL Simulation Results

File: test1.1_Trojan_Backdoor

Federated Learning Configuration

Total Clients (N): 2

Malicious Clients (M): 1

Neural Network: Test1.1_

Training Rounds: 2

Poisoned Rounds (R): 1

Distribution Strategy: first

Data Poisoning Attack Parameters

Poisoning Operation: backdoor_badnets

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using backdoor_badnets with 15.0% (0.15) intensity on 30.0% (0.30) of data for 1 rounds with 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9423

Poisoned Accuracy: 0.9473

Poisoned + DP Protection Accuracy: 0.0000

Drop (Clean - Poisoned): -0.0050

Drop (Clean - Init): -0.0022

Drop (Poisoned - Init): 0.0028

Drop (Poisoned DP - Init): -0.9445

DP Protection Method: trimmed_mean

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9425

Clean Recall: 0.9423

Clean F1 Score: 0.9424

Poisoned Precision: 0.9460

Poisoned Recall: 0.9459

Poisoned F1 Score: 0.9458

DP Protection Precision: 0.0000

DP Protection Recall: 0.0000

DP Protection F1 Score: 0.0000

Summary

FL Simulation Complete
Task: 3a0fa3eb-b57a-4702-b32f-61aef0122f9b
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9423
Poisoned Accuracy: 0.9473
Data Poison Protection Accuracy: 0.0000
Drop (Clean - Poisoned): -0.0050
Drop (Clean - Init): -0.0022
Drop (Poisoned - Init): 0.0028
Drop (Poisoned_DP - Init): -0.9445
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9425
Clean Recall: 0.9423
Clean F1 Score: 0.9424
Poisoned Precision: 0.9460
Poisoned Recall: 0.9459
Poisoned F1 Score: 0.9458
DP Protection Precision: 0.0000
DP Protection Recall: 0.0000
DP Protection F1 Score: 0.0000