FL Simulation Results

File: Semantic_Backdoor

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: semantic_backdoor

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using semantic_backdoor 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: 0.9458

Clean + DP Protection Accuracy: 0.9257

Poisoned Accuracy: 0.9450

Poisoned + DP Protection Accuracy: 0.9245

Drop (Clean - Poisoned): 0.0008

Drop (Clean - Init): 0.0013

Drop (Clean DP - Init): -0.0188

Drop (Poisoned - Init): 0.0005

Drop (Poisoned DP - Init): -0.0200

DP Protection Method: krum

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9459
Clean Recall: 0.9458
Clean F1 Score: 0.9457

Clean DP Precision: 0.9290
Clean DP Recall: 0.9257
Clean DP F1 Score: 0.9262

Poisoned Precision: 0.9451
Poisoned Recall: 0.9450
Poisoned F1 Score: 0.9449

DP Protection Precision: 0.9256
DP Protection Recall: 0.9245
DP Protection F1 Score: 0.9243

Summary

```
FL Simulation Complete
Task: c6387d6f-498b-4890-872c-086fe037057a
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9458
Clean DP Accuracy: 0.9257
Poisoned Accuracy: 0.9450
Data Poison Protection Accuracy: 0.9245
Drop (Clean - Poisoned): 0.0008
Drop (Clean - Init): 0.0013
Drop (Clean DP - Init): -0.0188
Drop (Poisoned - Init): 0.0005
Drop (Poisoned_DP - Init): -0.0200
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9459
Clean Recall: 0.9458
Clean F1 Score: 0.9457
Clean DP Precision: 0.9290
Clean DP Recall: 0.9257
Clean DP F1 Score: 0.9262
Poisoned Precision: 0.9451
Poisoned Recall: 0.9450
Poisoned F1 Score: 0.9449
DP Protection Precision: 0.9256
DP Protection Recall: 0.9245
DP Protection F1 Score: 0.9243
```