

FL Simulation Results

File: test2.2

Federated Learning Configuration

Total Clients (N): 10
Malicious Clients (M): 3
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 3 malicious clients.

Simulation Results

Init Accuracy: 0.7334
Clean Accuracy: 0.8618
Poisoned Accuracy: 0.6655
Poisoned + DP Protection Accuracy: 0.6078
Drop (Clean - Poisoned): 0.1963
Drop (Clean - Init): 0.1284
Drop (Poisoned - Init): -0.0679
Drop (Poisoned DP - Init): -0.1256
DP Protection Method: krum
GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8616

Clean Recall: 0.8618

Clean F1 Score: 0.8611

Poisoned Precision: 0.6810

Poisoned Recall: 0.6850

Poisoned F1 Score: 0.6771

DP Protection Precision: 0.6661

DP Protection Recall: 0.6178

DP Protection F1 Score: 0.6255

Summary

FL Simulation Complete

Task: 62016dd1-e545-460c-9b8d-facf60bd279e

GPU: GPU 0

Init Accuracy: 0.7334

Clean Accuracy: 0.8618

Poisoned Accuracy: 0.6655

Data Poison Protection Accuracy: 0.6078

Drop (Clean - Poisoned): 0.1963

Drop (Clean - Init): 0.1284

Drop (Poisoned - Init): -0.0679

Drop (Poisoned_DP - Init): -0.1256

Data Poison Protection Method: krum

--- Confusion Matrix Metrics (Weighted Avg) ---

Clean Precision: 0.8616

Clean Recall: 0.8618

Clean F1 Score: 0.8611

Poisoned Precision: 0.6810

Poisoned Recall: 0.6850

Poisoned F1 Score: 0.6771

DP Protection Precision: 0.6661

DP Protection Recall: 0.6178

DP Protection F1 Score: 0.6255