Report Social Network

Name : Ahmed emad Fawzy moahmmed

ID : 2205086

DR : Reem essam

Eng : Marwan

Introduction

This experiment focuses on detecting bot accounts inside a social network graph derived from the Facebook dataset.
The workflow includes:

- Graph loading
- Graph sampling for faster processing
- Feature extraction
- Baseline bot classification
- Two adversarial attacks: Structural Evasion & Graph Poisoning
- Performance comparison before and after attacks

Graph Construction

The original dataset contains:

- Nodes: 4039
- Edges: 88234

To ensure fast computation, the graph was reduced using BFS sampling to:

- Nodes: 800
- Edges: 7448

Feature Extraction

The following graph metrics were computed for each node:

- Degree
- Clustering Coefficient
- PageRank
- Closeness Centrality
- Betweenness Centrality
- Eigenvector Centrality
- Community ID (Louvain)

Bot Label Assignment

To simulate malicious accounts:

- **5%** of the nodes (40 bots out of 800) were randomly selected as bot accounts. These bots were used to train and test a Random Forest classifier.

Baseline Classification Result

Model used: **RandomForestClassifier (150 trees)**

Baseline Results (No Attack)

- Accuracy: 0.99375
- Model detected bots strongly before any adversarial manipulation.

Output:

Baseline Accuracy

0.99375

precision recall f1-score support

0 → 0.99   1.00   1.00   760

1 → 1.00   0.88   0.93   40

Structural Evasion Attack

Bots attempt to avoid detection by **removing edges**, decreasing their visibility in the graph.

Results After Evasion Attack

- Accuracy: 0.94875
- Bots became harder to detect → the model predicted nearly all nodes as humans.
  Accuracy: 0.94875
  Bots F1-score drops to 0.00 (model cannot detect bots)

  Graph Poisoning Attack
  Bots create edges with highly-connected nodes (top 100 high-degree users) to blend with real human patterns.
   Results After Poisoning Attack
- **Accuracy:** 0.95
- Model again fails to identify bots → heavy decrease in bot precision & recall.
  Output:
  After Graph Poisoning
  Accuracy: 0.95
  Bots precision = 0.00, recall = 0.00

Original Sampled Graph

After Graph Poisoning Attack