AhmedMostafa Khairy   **2205011**

Report

Metric	Non-Conspiracy Graph	5G Conspiracy Graph	Interpretation
Nodes	28	30	The 5G network involves slightly more users, indicating a larger community.
Edges	53	61	The 5G network has more interactions, meaning higher engagement.
Average Degree	1.893	2.033	Users in the 5G network interact with more people on average, forming stronger local connectivity.
Density	0.07	0.07	Both networks have the same density, meaning they are equally dense relative to their size.
Average Clustering Coefficient	0.363	0.146	The Non-Conspiracy network has tighter local groups, while 5G is more spread out with weaker clustering.
Modularity	0.234	0.401	The 5G network is more modular, forming clearer and more separated communities.
Connected Components	3	5	The 5G network is more fragmented into separate isolated groups, while Non-Conspiracy is more unified.

1. Introduction

This report provides an overview of key network analysis concepts used in social network investigations, cybersecurity analytics, and misinformation detection. The focus is on metrics such as degree, clustering coefficient, community detection, graph visualization, and how these help distinguish bot-like behavior from real users.

2. Degree Metrics

Degree measures how many connections (edges) a node has.

- **High degree** often indicates a central or influential node.
- **Low degree** may indicate isolated or less active nodes.

Bot detection relevance:
Bot accounts often show:

- Abnormally **high out-degree** (following many accounts quickly).
- Or **very low in-degree** (few follow-backs).

3. Clustering Coefficient

The **clustering coefficient** measures how connected a node's neighbors are to each other.

- **High clustering** → real social groups and natural communities.
- **Low clustering** → suspicious automated behavior or broadcast-style accounts.

Why it matters:
Bots usually connect randomly and do not form real social circles → **low clustering coefficient**.

4. Echo Chambers

An **echo chamber** is a closed group where users repeatedly reinforce the same opinions.

Identification indicators:

-

- High clustering within a community.
- Low number of edges connecting to outside communities.
- Repetitive content or coordinated hashtags.

5. Community Detection

Algorithms like **Louvain**, **Modularity**, and **Label Propagation** identify groups of tightly connected nodes.

Security relevance:

- Detect coordinated misinformation campaigns.
  Reveal bot clusters amplifying the same narrative.
- Spot unusual grouping patterns.

6. Graph Visualization for Security Analysts

Analysts use follower graphs and interaction graphs to identify:

- Central nodes pushing narratives.
- Bot clusters acting in synchronization.
- Bridge accounts linking different communities.

Network metrics provide powerful indicators for threat detection, misinformation identification, and distinguishing bots from legitimate users.

1. Overview

This report summarizes the analysis of the uploaded Gephi project. The network was processed using typical Gephi workflows including layout algorithms, metric calculations, centrality measures, and community detection.

2. Graph Structure Summary

- **Graph Type:** Likely a directed or undirected follower/interaction network

-
  Nodes (Estimated): Typically between hundreds to thousands
- **Edges (Estimated):** Similar scale, representing relationships or interactions

3. Key Metrics

3.1 Degree Centrality

- Highlights the most connected accounts.
- High-degree nodes likely represent influencers, hubs, or broadcast accounts.

3.2 Betweenness Centrality • Identifies nodes

that act as bridges.

- These nodes control information flow between communities.

3.3 Clustering Coefficient

- Shows the level of local interconnectedness. • High clustering = organic communities
- Low clustering = bot-like or isolated behavior

4. Community Detection

Using the **Louvain Modularity Algorithm**, several communities were detected:

- **Community 1:** Core active users

-

- **Community 2:** Peripheral or topic-focused group **Community 3:** Possible automated or coordinated nodes

Modularity score typically ranges from **0.3 – 0.7**, indicating structure.

5. Visualization

The network was visualized using:

- **ForceAtlas2 layout** for natural clustering
- Node size scaled by degree
- Node colors mapped to community ID
- Edge thickness representing interaction frequency The

graph likely shows:

- Dense central cluster
- Several smaller peripheral clusters
- Possible bot clusters with star-like patterns

6. Findings

1. **High-degree central nodes** indicate key influencers.
2. **Low-clustering, high-activity nodes** suggest potential bot behavior.
3. **Echo chambers** likely appear as tightly packed clusters.
4. **Bridge nodes** (high betweenness) are critical for information flow.