Comparing Malicious vs. Benign Twitter Subgraphs

A Social network Project

Presented by:

Omar hossam Ahmed

2205150

Objective:

To analyze the 2 communities and compare them in the context of security and get a closer look of their structure.

First, Defintions :::

1. Number of Nodes and Edges

Definition:

- **Nodes** represent accounts (users).
- **Edges** represent interactions/connections (e.g., follow, retweet, mention).

Example:
If your graph has **96 nodes** and **3094 edges**, it means:

- There are 96 Twitter accounts involved.
- Between them, 3094 interactions exist.

2. Average Degree

Definition:
The **average number of connections per node**.

- In **directed graphs**, degree = indegree + outdegree.

Example:
If the network has average degree = **64**, each user is connected to ~64 others on average.

3. Graph Density

Definition:
How "full" the graph is. It measures the **ratio of existing edges to all possible edges**.

- Ranges from **0 to 1**.
- Higher density = more interconnected graph.

Example:
Density = **0.3**
→ 30% of all possible user connections actually exist.

Note :: Conspiracy networks often have **higher density** because misinformation accounts amplify each other.

4. Average Clustering Coefficient

Definition:
Measures **how often a node's neighbors are also connected to each other**.

- High clustering = tight groups / echo chambers
- Low clustering = more open, diverse network

Example:
Clustering = **0.72**
→ If A, B, C follow each other, A's neighborhood forms a triangle → very clustered.

Note :: Conspiracy networks usually have **high clustering** (closed echo chambers).

5. Modularity (Q) and Number of Communities

Definition:
Modularity detects **clusters (communities)** in the graph and measures how separated these groups are.

- **Q ranges from –1 to 1**
- Higher Q = clearer, more distinct communities.

Example:
Modularity Q = **0.64**, communities = **4**
→ The network has four well-defined groups who mostly talk inside their own cluster.

Note :: Conspiracy networks often show **higher modularity**, meaning clear ideological factions.

6. Betweenness and Closeness Centrality

Betweenness Centrality

Definition:
Measures how often a node lies on **shortest paths** between other nodes.
→ Identifies **brokers**, **influencers**, or **bridge accounts**.

Example:
If one node has very high betweenness:
→ It acts as a bridge connecting two communities.

Closeness Centrality

Definition:
Measures how quickly a node can reach all others in the network.
→ Identifies **core users**, **spreaders**, or **influencers**.

Example:
A node with high closeness can spread information fastest.

7. Connected Components

Definition:
A connected component is a **subgraph where all nodes are reachable from each other**.

In directed graphs Gephi calculates **weakly connected components** by default.

Example:
If the graph has **1 component**, all accounts are indirectly connected.
If it has **3 components**, the network is split into 3 isolated subgraphs.

Note :: Misinformation networks tend to form **one giant connected component** because they reshared heavily.

BENIGN GRAPH ANALYSIS (g_norm)

Dataset overview

- **Nodes:** 48 (from the rows shown)
- **Directed edges:** High volumes but distributed more evenly
- This graph corresponds to a *normal, non-misinformation* sub-community.

1. Degree Distribution

Nodes exhibit a healthy, organic degree distribution:

Degree Type	Observation
Low degree nodes (0–3): Many	These represent normal passive accounts, not bots
Medium degree nodes (5–15): Majority	Normal users engaging moderately
High degree (20–60+): Few hubs	Natural influencers

The **highest degree = 61** (node `210910383`)

Interpretation:
A **heterogeneous** degree distribution indicates **organic behavior**. No sign of Sybil clusters (which usually have dozens of nodes with extremely similar degrees).

2. Clustering Coefficient

Clustering values range from **0 to 1**, with many nodes around:

- **0.3–0.7** = moderate clustering
- Indicates natural conversational subgroups
- No extremely tight clusters where every node connects to every node (a red flag for fake engagement rings)

Interpretation:
Benign Twitter communities have moderate clustering. Misinformation clusters show **much higher and more uniform clustering** because bot rings retweet each other.

3. Centrality Measures

3.1 Closeness Centrality

Most nodes have:

- closeness = **0.4–0.55**
- indicating healthy "small-world" connectivity.

High closeness nodes:

- `299376005` (0.578)
- `31861159` (0.506)
- `28058172` (0.616)
- `210910383` (0.880) ← **the global hub**

High closeness is normal for influencers, not suspicious.

3.2 Betweenness Centrality

Only a few nodes show high betweenness:

- 31861159: **180.48**
- 28058172: **161.93**
- 208274276: **152.18**
- 210910383: **905.7** ← dominant bridge

Interpretation:
Benign networks usually show a **few natural bridges** connecting communities.
Misinformation graphs show **many evenly distributed betweenness peaks**, because bots coordinate information flow.

4. Modularity & Communities

The graph shows **7 or more modularity classes**:

- modularity_class = 0,1,2,3,4,5,6,7

This means:

- Many communities
- Loose topics
- Healthy diversity
- No “super-cohesive” echo chamber

Interpretation:
Benign networks are **topic-diverse**.
Conspiracy networks typically have **1–2 huge communities**, because misinformation spreads in echo chambers.

5. Connected Components

Column `componentnumber` shows many small weakly connected components:

- Values: 0,1,2,3,4,5— up to 8
- No single dominant mega-cluster
- No artificial cliques

Interpretation:
Benign graphs have **fragmentation** and **isolated users**.
Misinformation graphs have **one extremely large connected giant component** and sometimes many tiny fake ones.

6. Behavioral Attributes (friends / followers)

Nodes have:

- **friends: 7–15**
- **followers: 7–15**
- Narrow but realistic range
- No extreme asymmetry (e.g., 2000 friends, 0 followers — a red flag for fakes)

This is **normal human behavior**.

Interpretation:
Benign network → balanced social metrics
Misinformation network → many accounts with:

- low followers
- high outdegree
- abnormal friend/follower asymmetry
- “burst” activity

7. Suspicious Accounts Check

Graph contains:

No obvious Sybil nodes

- No clusters of degree 1–3 with highly similar attributes
- No nodes with abnormal friend/follower imbalance
- No nodes with betweenness = 0 and outdegree = 0 in large groups
- No copy-patterns in time attribute

Everything looks organic.

MALICIOUS GRAPH ANALYSIS (g_misinfo)

1. Overview

This graph represents a misinformation-oriented Twitter community that engages with 5G-related conspiracy content. The network shows strong signs of **centralized influence**, **coordinated behavior**, and possible **inauthentic accounts** (Sybil-like nodes), indicating the presence of artificially amplified misinformation dynamics.

2. Structural Metrics

2.1. Number of Nodes and Edges

- **Nodes:** 96

- **Edges:** 3094
  The high ratio of edges to nodes indicates **intense interaction**, which is a known pattern in misinformation networks where accounts frequently retweet or mention each other to amplify content.

2.2. Average Degree

- **Avg. Degree:** (In + Out) ~ 64
  This is extremely high for only 96 nodes. It suggests:
- Heavy cross-interaction
- Possible retweet-bots or coordinated accounts
- Echo-chamber behavior

2.3. Graph Density

- **Density:** Very high for a directed graph of this size
  High density supports the idea of **tightly interconnected accounts** forming a reinforcement loop.

2.4. Average Clustering Coefficient

Most nodes have clustering between **0.7 – 0.9**
This is unusually high and indicates:

- Closed triads
- Repeated interactions among the same accounts
- Potential coordination or scripted retweet chains

Misinformation networks typically show **higher clustering** than normal communities.

2.5. Modularity (Q)

- **Modularity classes:** 5
- **Modularity Q value:** Low–moderate (expected with dense graphs)

Low modularity means:

- Communities are **not well separated**
- The network behaves more like a **single coordinated block**
  This is again consistent with misinformation networks.

2.6. Centrality Measures

Betweenness Centrality

Several nodes stand out with extremely high betweenness, e.g.:

- **13276280** → 552
- **58424389** → 305
- **27990901** → 353
- **43835**, **44011**, **34346603**, **25024383** → 150–300+

These are likely:

- **Influencers / key amplifiers**
- **Bridge nodes** that connect subclusters
- Accounts responsible for content propagation

Closeness Centrality

Most nodes have closeness values around **0.65–0.85**, meaning:

- Every node is only **1–2 steps away** from the rest
- Extremely tight communication radius

This is not normal for organic communities.

2.7. Connected Components

- **Weakly Connected Components:** 1
- **Strongly Connected Components:** 5+ small SCCs
  The giant WCC indicates:
- A single community dominated by internal interaction

Small SCC clusters may represent:

- Retweet bots
- Suspicious pairs
- Small amplification loops

3. Suspicious Activity (Sybil / Fake / Coordinated Accounts)

From the data:

- Most accounts have **very similar friends & followers values (12–17)**
- Many nodes have **outdegree ≈ indegree (balanced)**
- Several show:
  - High connectivity
  - Very high betweenness despite small profile numbers
  - Perfect clustering (1.0)
  - Strongly synchronized behavior

These are indicators of:

✓ **Coordinated Sybil-like activity**

✓ **Bot-assisted retweet amplification**

✓ **Fake follower clusters**

Nodes with **Degree > 120**, **Closeness > 0.80**, and **Betweenness > 200** are especially suspicious since real users rarely show such perfect alignment.

4. Key Observations (Misinformation Cluster Behavior)

1. **Extremely interconnected structure**
   Indicates a coordinated group rather than an organic conversation.
2. **High clustering + low modularity**
   Suggests a "tight bubble" — typical echo-chamber.
3. **High centrality hubs**
   These likely function as:
   a. Main misinformation spreaders
   b. Bots amplifying each other
   c. Fake high-impact accounts
4. **Suspicious accounts detectable through heuristics**
   a. Near-identical metadata (friends/followers)
   b. High degrees despite low profile metrics
   c. Zero eccentricity in some nodes
   d. Perfect clustering values
5. **Bot-like retweet chains**
   Many nodes have around **50–70 in/out edges**, forming radial patterns around central influencers.

5. Conclusion

This misinformation subgraph shows all the classic signatures of **coordinated inauthentic behavior**:

- High density
- High clustering
- Centralized influencers
- Suspicious nodes with identical metadata
- Low modularity
- High betweenness “super nodes”

Compared to a **benign** cluster:

- The benign network is more distributed, less dense, and has more natural variation
- The misinformation network is almost **machine-like** in its symmetry and structure

This makes misinformation clusters easier to detect using network metrics and suspicious-node labeling.

The most suspicious nodes fall into two categories:

1. Sybil / Fake / Low-quality Accounts

Identified by:

- degree = 0
- followers < 5
- friends < 10
- isolated components

Examples:

- **814803462**
- **107660002**
- **151569267**

2. High-power Coordinated Amplifiers

Identified by:

- extremely high degree (> 110)
- very high betweenness (> 150)
- high closeness
- high modularity class centrality

Examples:

- **27990901** (highest betweenness)
- **13276280**
- **58424389**
- **67498674**
- **145456298**

These nodes behave like **core influencers or automated propagation accounts** spreading content across communities.

COMPARISON: BENIGN vs. MISINFORMATION GRAPH

Feature	Benign Graph	Conspiracy Graph
Degree distribution	Wide & natural	Often polarized (many low-degree bots + a few hyper-hubs)

Clustering coefficient	0.3–0.7 moderate	Very high in bot “echo ring” clusters
Communities	Many small communities (5–10+)	1–2 giant communities (echo chamber)
Betweenness	Few natural influencers	Many nodes with suspiciously high betweenness (coordination)
Connected components	Several	Usually one giant component pushing misinformation
friends/followers symmetry	Balanced	Low followers, high outdegree typical of bots
Sybil signals	None	Present in many conspiracy subgraphs
Graph shape	Organic, spaced, multi-topic	Dense core + bot periphery (“starburst” pattern)