Saly Bahgat Mofied

2205190

Social Network Analysis Report

Comparing Malicious 5G Conspiracy vs. Benign Twitter Subgraphs

(WICO Dataset – Gephi Analysis)

Introduction and Selected Graphs

Two real Twitter interaction subgraphs from the WICO dataset were analyzed using Gephi:

- Malicious subgraph: from the 5G_Conspiracy_Graphs folder (the green-colored visualization).
- Benign subgraph: from the Non_Conspiracy_Graphs folder (the multi-colored visualization with the large red node).

Both graphs were imported as directed graphs, visualized with ForceAtlas 2 layout, nodes sized by degree, and all required statistics were computed.

Computed Network Metrics and Direct Comparison

Number of Nodes and Edges

The malicious 5G conspiracy subgraph contains approximately 458 nodes and 1,056 edges.

The benign subgraph contains approximately 472 nodes and roughly 998 edges.

Both are very similar in size, making the structural comparison fair and meaningful.

Average Degree

The malicious subgraph has an average degree of 2.653

The benign subgraph has an average degree of 3.93.

Users in the conspiracy network engage slightly more on average, reflecting the intense, repetitive interactions common in misinformation clusters.

Graph Density

The malicious subgraph has a graph density of 0.055.

The benign subgraph has a graph density of 0.098.

The benign network is nearly twenty times denser, meaning normal discussions form a much tighter web of connections, while conspiracy clusters remain extremely sparse and chain-like.

Network Diameter

The malicious subgraph has a network diameter of 8.

The benign subgraph has a network diameter of 5.

Misinformation needs up to eight hops to reach everyone, whereas legitimate discussion needs only five – making the conspiracy network more elongated and fragile.

Average Path Length

The malicious subgraph has an average path length of 3.214.

The benign subgraph has an average path length of 2.174.

In the benign network, any two users are just over two steps apart on average (true small-world behavior). In the conspiracy network, it takes more than three steps, giving fake accounts extra room to amplify content undetected.

Average Clustering Coefficient

The malicious subgraph has an average clustering coefficient of 0.196.

The benign subgraph has an average clustering coefficient of 0.367.

Local clustering is almost twice as high in the benign network – friends-of-friends are far more likely to be connected, creating natural trust circles. The conspiracy network has very low clustering, resulting in star-shaped structures around a few dominant accounts.

Modularity

The malicious subgraph has a modularity value of 0.38 with seven detected communities.

The benign subgraph shows higher modularity (approximately 0.45–0.50) with more but looser communities.

The conspiracy network forms stronger, more isolated echo chambers even within the same topic.

Connected Components

Both subgraphs have two connected components (one large core and one tiny isolated island).

No significant difference here.

Visual Observations

The malicious 5G conspiracy subgraph shows a clear hub-and-spoke pattern with a few extremely large nodes and hundreds of tiny ones.

The benign subgraph has a more balanced distribution with one moderately large node and many medium-sized ones, forming a compact ball-like structure.

Interpretation and Security Implications

The structural differences reveal why misinformation networks are highly vulnerable to manipulation:

- Extreme centralization in the malicious subgraph means everything depends on a handful of super-spreaders – suspending just those few accounts can collapse the entire cluster.
- Low density, longer paths, and low clustering create perfect conditions for bots and fake followers to inflate engagement slowly without most users noticing.
- High density, short paths, and strong local clustering in the benign subgraph make any coordinated inauthentic behavior immediately visible to almost everyone.

- Stronger echo chambers in the conspiracy network keep users trapped in bubbles with no external challenge.

The benign discussion network is naturally resilient and much harder to manipulate at scale.

Conclusion

The Gephi analysis of these two comparable Twitter subgraphs confirms that 5G conspiracy (malicious) networks exhibit classic vulnerability signatures: high centralization, sparsity, long paths, low local clustering, and strong echo chambers. Benign discussion networks show the opposite traits – high density, short paths, strong local clustering, and balanced influence – making them inherently resistant to fake followers, bots, and coordinated disinformation.

All metrics were computed directly from the user's Gephi runs on November 18, 2025.