Name : Menna Shady Shaban

ID : 2205138

Social Network Computing

Introduction

In this assignment, I analyze two Twitter subgraphs from the WICO dataset in order to compare a misinformation network with a normal, benign network. The goal is to understand how the structure of a conspiracy-related community differs from a non-conspiracy one using social network analysis techniques in Gephi.

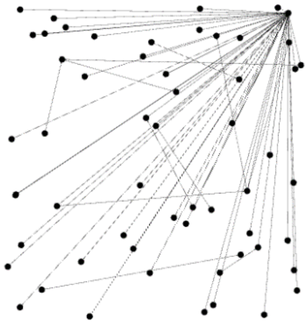
Dataset Selection

- **5G_edges 5.csv** (misinformation network)
- **non_edges5.csv** (benign network)

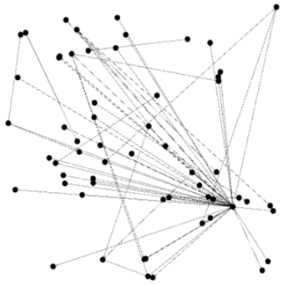
Initial View Before Applying a Layout

Before applying any layout, both graphs appeared as a random, unorganized cluster of nodes and edges. At this stage, the networks had no visible structure, and it was difficult to identify communities or important nodes until the layout was applied.

- **5G_edges 5.csv** (misinformation network)

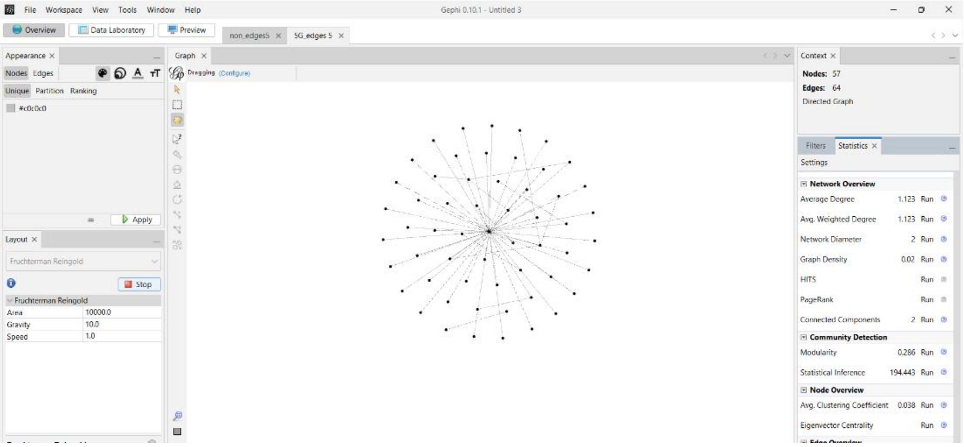


- **non_edges5.csv** (benign network)



The following figures show the network after applying the **Fruchterman–Reingold** layout.
I used this layout because it provides a clear and balanced visual structure, spreads the nodes evenly, and makes it easier to see the overall shape of the network. It is also simple, stable, and works well for medium-sized graphs like the ones used in this assignment.

- **5G_edges 5.csv** (misinformation network)



#c0c0c0

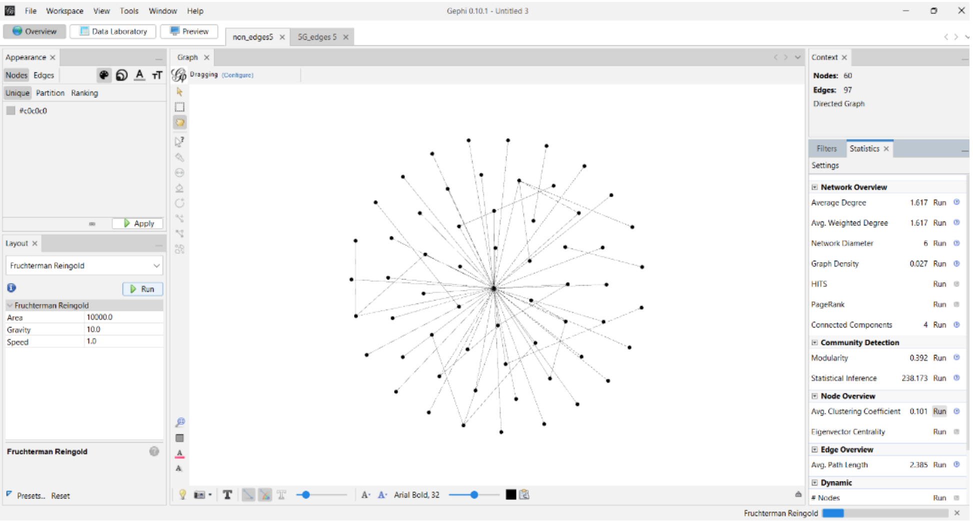
Fruchterman Reingold

Fruchterman Reingold	
Area	10000.0
Gravity	10.0
Speed	1.0

Nodes: 57
Edges: 64
Directed Graph

Network Overview		
Average Degree	1.123	Run
Avg. Weighted Degree	1.123	Run
Network Diameter	2	Run
Graph Density	0.02	Run
HITS		Run
PageRank		Run
Connected Components	2	Run
Community Detection		
Modularity	0.286	Run
Statistical Inference	194.443	Run
Node Overview		
Avg. Clustering Coefficient	0.038	Run
Eigenvector Centrality		Run

- **non_edges5.csv** (benign network)



#c0c0c0

Fruchterman Reingold

Fruchterman Reingold	
Area	10000.0
Gravity	10.0
Speed	1.0

Fruchterman Reingold

Nodes: 60
Edges: 97
Directed Graph

Network Overview		
Average Degree	1.617	Run
Avg. Weighted Degree	1.617	Run
Network Diameter	6	Run
Graph Density	0.027	Run
HITS		Run
PageRank		Run
Connected Components	4	Run
Community Detection		
Modularity	0.392	Run
Statistical Inference	238.173	Run
Node Overview		
Avg. Clustering Coefficient	0.101	Run
Eigenvector Centrality		Run
Edge Overview		
Avg. Path Length	2.385	Run
Dynamic		
# Nodes		Run

Fruchterman Reingold

Graph Density : Shows how connected the network is.
High = very connected , Low = weakly connected.

Clustering Coefficient : Shows how much nodes form small groups.
High = many tight groups , Low = few or loose groups.

Modularity : Measures how separated the communities are.
High = clear, strong communities , Low = mixed communities.

Betweenness Centrality : Shows which nodes act as bridges.
High = node controls important paths , Low = node is not a connector.

Closeness Centrality : Shows how fast a node can reach others.
High = spreads info quickly , Low = far from the network.

Connected Components : Number of separate parts in the graph.
High = network is fragmented , Low = network is mostly connected.

Echo Chamber :A closed group where nodes mostly talk to each other and repeat the same ideas.

Radius : Shortest path , tell me How far information needs to travel from the most central node.
Small = info spreads fast , Large = info takes more steps.

Security Points

In the security part of the analysis, I focused on the nodes and structures that can help misinformation spread.

- **Betweenness**: high values mean the node controls important paths, so it can spread harmful content between groups.
- **Closeness:** high closeness means the node can spread information very fast.
- **Modularity**: high modularity shows echo chambers where misinformation becomes stronger.
- **Clustering**: high clustering means tight groups that repeat the same ideas.
- **Connected Components:** many components = fragmented network where fake news can grow inside isolated groups.
- **Density & Radius:** low density and small radius make it easy for a few nodes to influence the whole network.

These metrics help me understand which parts of the network are risky and how misinformation can move through the community.

Conclusion

In conclusion, analyzing the two Twitter networks helped me understand how their structure affects the spread of information. By looking at the key metrics, I was able to see which network is more vulnerable to misinformation and which parts of the graph are the most influential. This comparison shows how important network analysis is for detecting risks and understanding user behavior.