Name: Jana Adel Ramadan ID: 2205105

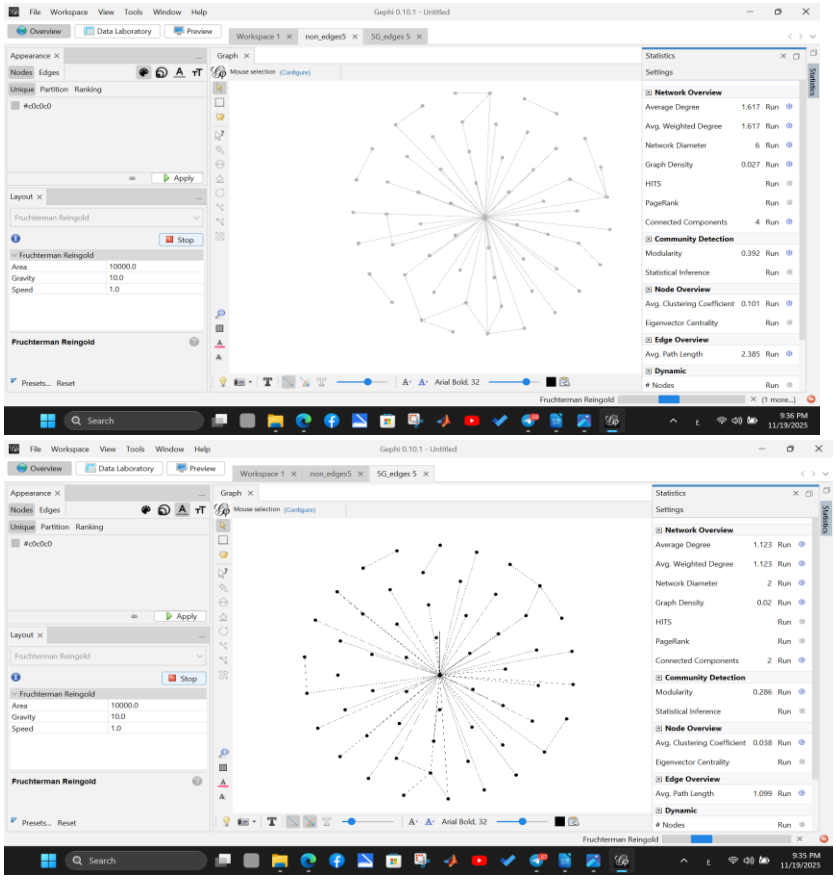
Social Network

Introduction

We analyzed two Twitter subgraphs extracted from the WICO Dataset: one representing a misinformation (5G conspiracy) cluster, and another representing a normal (non-conspiracy) community. Using Gephi, we compute key network measures such as degree, clustering coefficient, density, modularity, centrality metrics, and connected components. By comparing these metrics, we highlight the structural differences between malicious and benign communities and explain how these findings enhance our understanding of misinformation diffusion and social network security.

Comparing Malicious vs. Benign Twitter Subgraphs (WICO Dataset)

1. Choose from graph 5G_Conspiracy_Graphs num 5 and from Non_Conspiracy_Graphs num 5.
2. Apply in Gephi.



3.

Metric	5G_Conspiracy	Non-Conspiracy	Interpretation
Average Degree	1.123	1.617	The normal network is more connected between users
Connected Components	2	4	Natural society is more fragmented and decentralized.
Graph Density	0.02	0.027	The normal network (non-conspiracy) has more links between users.
Network Diameter	2	6	The highly centralized misinformation society (5G_Conspiracy).
Avg. Clustering Coefficient	0.038	0.101	A normal society has more social clusters and greater interaction between neighbors.
Modularity (Q)	0.286	0.392	-The normal network (non-conspiracy) contains multiple, balanced groups. -5G graph the network is clustered around a single source (echo chamber).
Communities	Low	High	

Betweenness Centrality

- It is a measure that determines the extent to which a node acts as an "intermediary" or "bridge" between the other nodes in the network.
- A node with high interconnection is one through which the shortest paths between other users pass.
- In misinformation networks (5G conspiracies):

Accounts with high Betweenness are the primary bots, deleting or disabling these accounts leads to a complete network crash.

Closeness Centrality

- Closeness is a measure of how close a node is to all other nodes in the network.
- The fewer the hops between a node and the rest of the network, the higher the closeness
- In misinformation networks, accounts with high closeness are often those that can quickly disseminate content with wide reach.
  High closeness helps in identifying "influencers" within the network.
  Low closeness may indicate that the user is peripheral and unimportant.

Importance of network analysis as a Cyber Security Specialist

1. Detecting coordinated misinformation campaigns
2. Understanding attack techniques in social engineering
3. Supporting threat intelligence platforms
4. Identifying botnets and their impact
5. Protecting businesses from harmful viral content
6. A core component of OSINT (Open-Source Intelligence)

Conclusion

The WICO Twitter subgraph analysis demonstrates that misinformation networks exhibit distinctive structural patterns that separate them clearly from normal social graphs. Misinformation clusters tend to be centralized, low-clustering, and dominated by a few influential nodes, while benign networks show more balanced connections and stronger community structures. Through metrics such as centrality, modularity, and graph density, we can identify suspicious behavior, detect coordinated bot activity, and understand how harmful content propagates.