

Anomaly Detection

Mike Tsamis and Maria Taranov

Mentor: Dr. James Abello

Anomaly Detection

- Network anomalies typically refer to circumstances when network traffic deviates from normal network behavior.
- Anomaly detection involves analyzing and comparing datasets in order to assess network patterns which are deemed “normal” or “abnormal”.

Graph Visualization

- Networks are often represented by very large graphs that can consist of millions of edges and nodes, so graph visualization software is often used to view, analyze and interact with graphs.
- Interactions include reducing depth, labeling nodes, and clustering the overall graph.
- Examples of Graph Visualization software: Cytoscape and ASK-GraphView.



Locale

1999

Page 10

— netherlands the of in holland peopl

- animals the (2)
- netherlands currency (2)
- culture netherlands (4)
- netherlands timeline (4)
- agriculture the (3)
- netherlands drugs (2)
- netherlands animals
- currency of the netherlands
- culture of the netherlands
- holland history
- netherlands timeline
- netherlands transportation
- netherlands agriculture
- drugs in the netherlands
- attractions (2)
- facts (2)

✳ COMPONENTS (15)

* COMPONENTS (75)



netherlands the holland is of what (S). SIZE: 46. WEIGHT: 162. DEGREE: 7. ID: 4770_MCLCLUSTERH-2 (3) (6653). SCALE: 0.0485955763667754. MRVS:



Our Project

- This project addresses the problem of finding persistent patterns in evolving networks. A central question is the characterization of patterns that can be used as the basis to detect anomalous activities in time-evolving networks.
- One of the datasets we will be working with is from Twitter.

Examples from Twitter



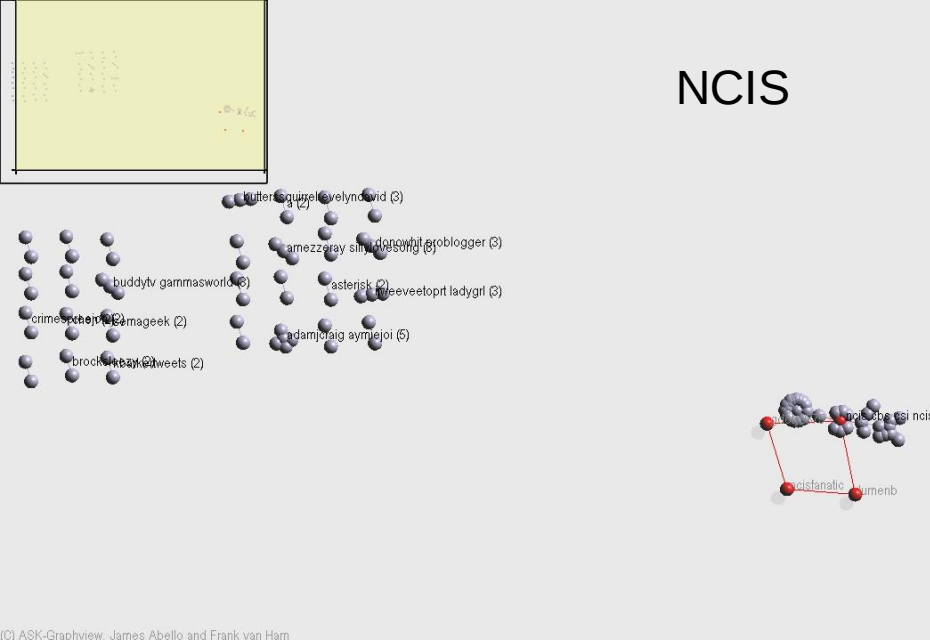
@stevenlambert44

Steven Lambert

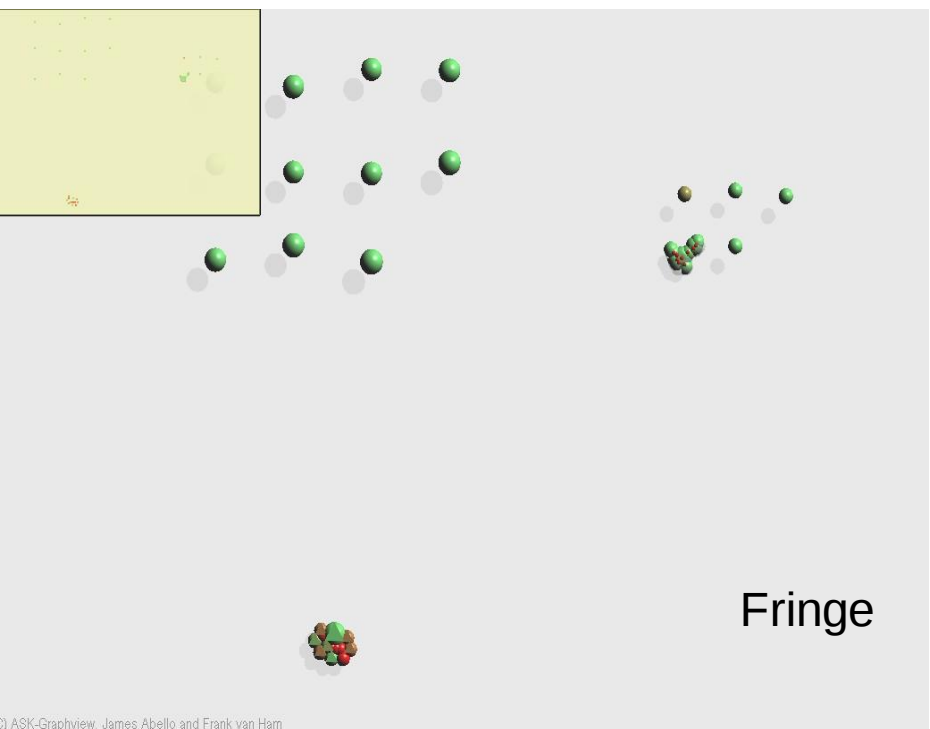
I'd vote sue! RT @SteveR_664
Career in politics now going. Vote
Sue #Glee

27 minutes ago via TweetCaster

NCIS



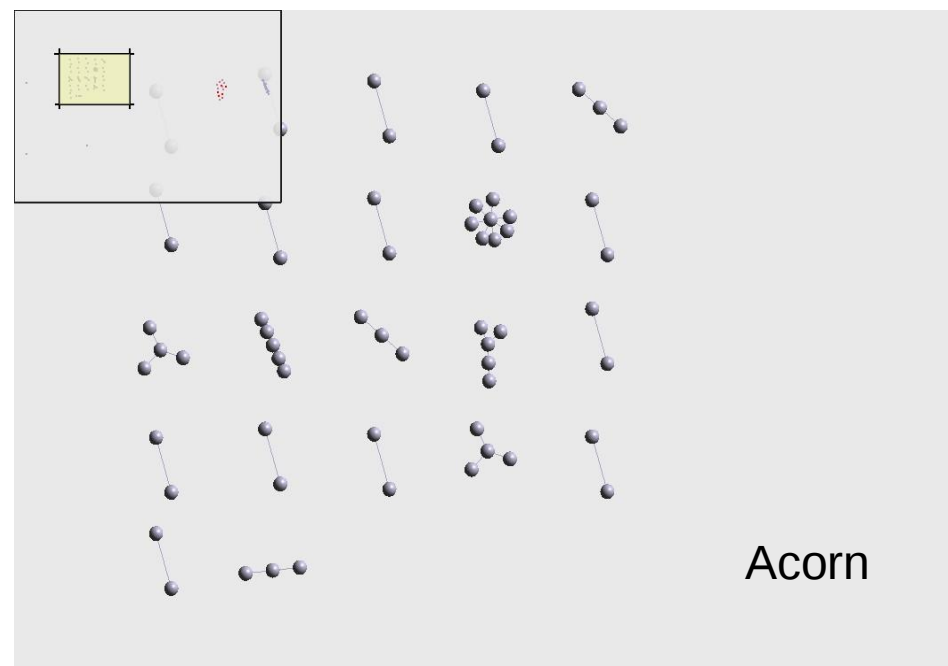
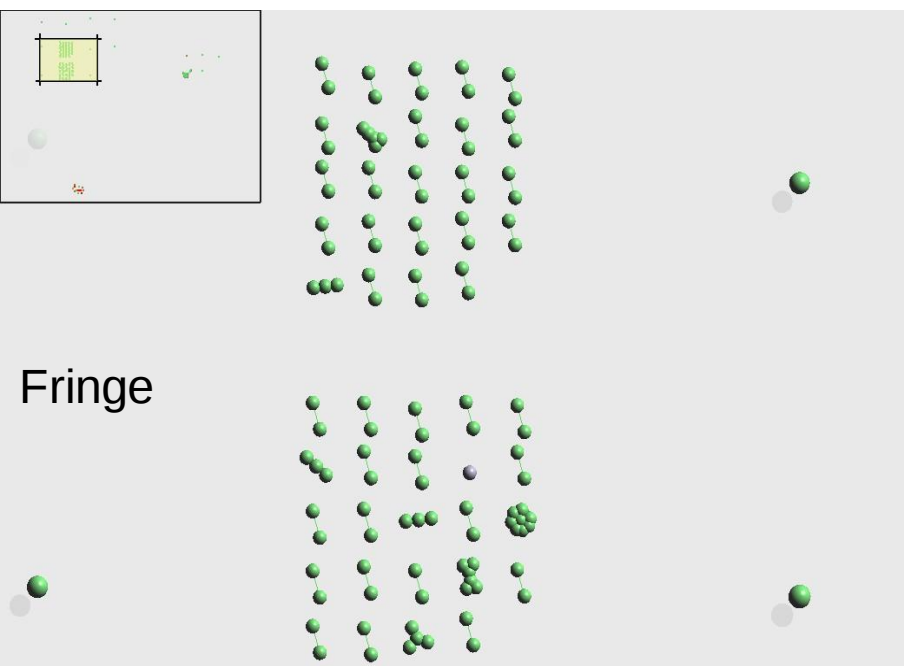
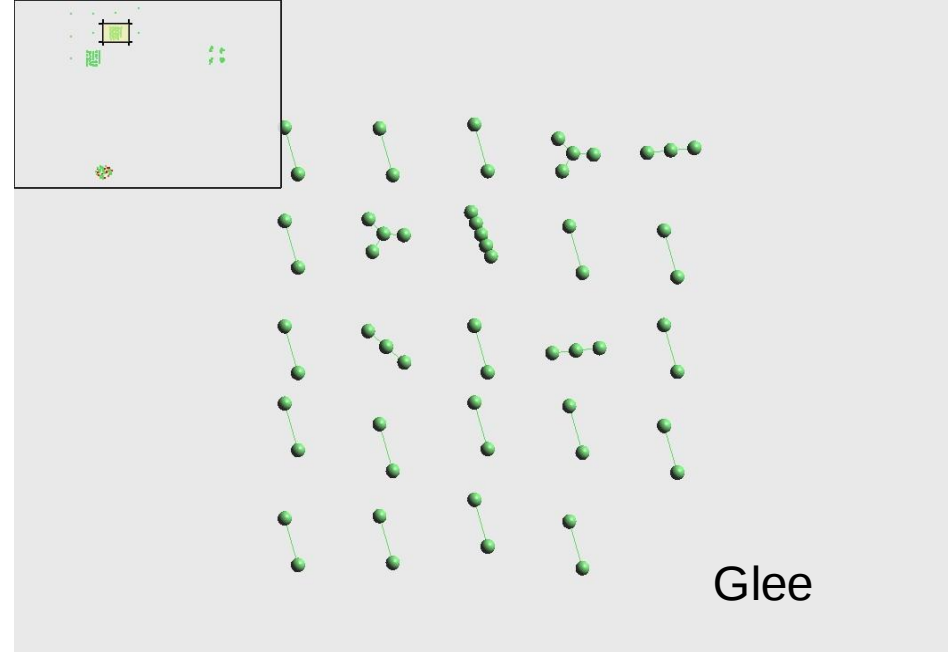
Glee

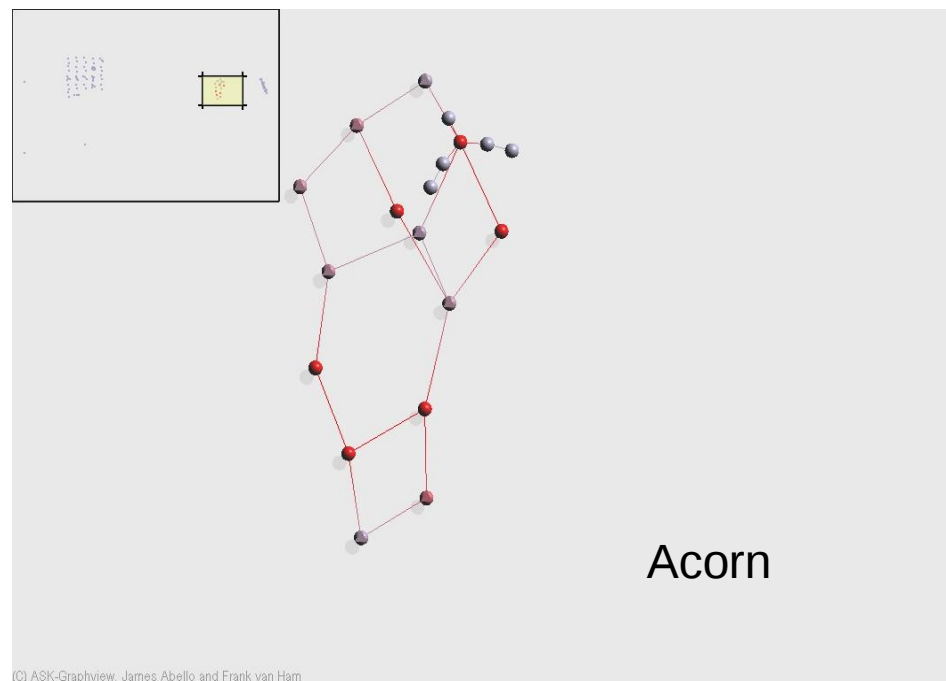
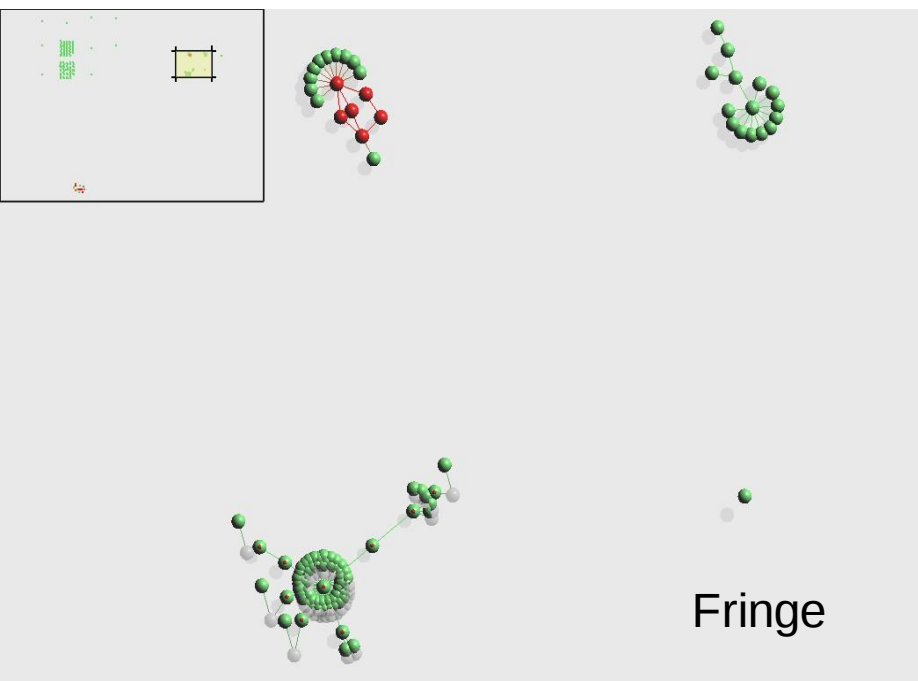
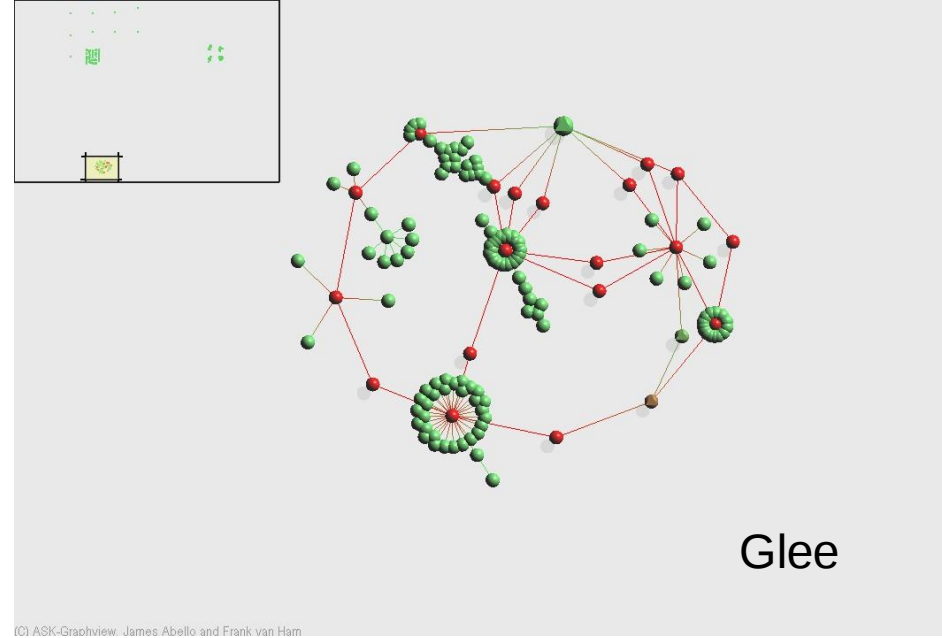
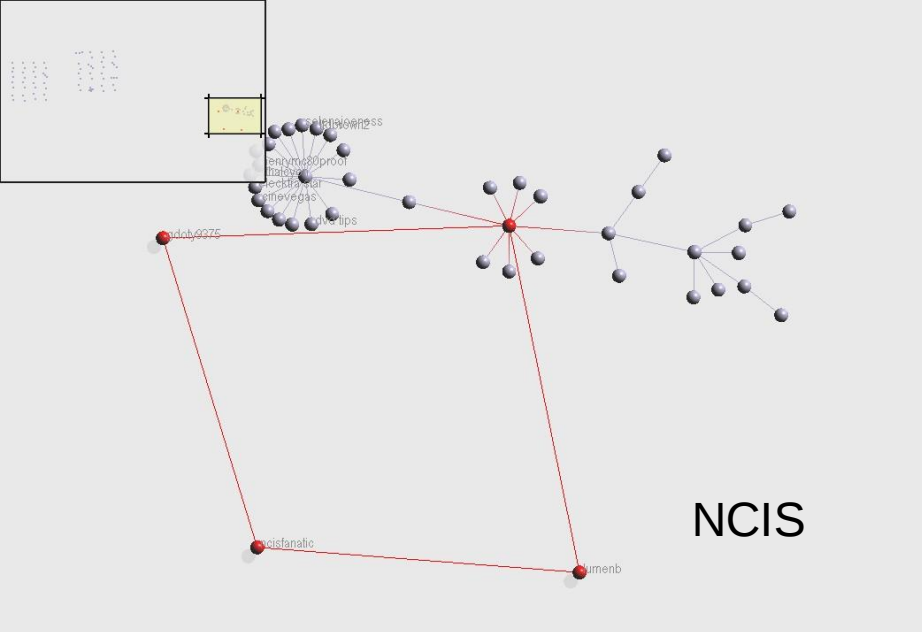


Fringe

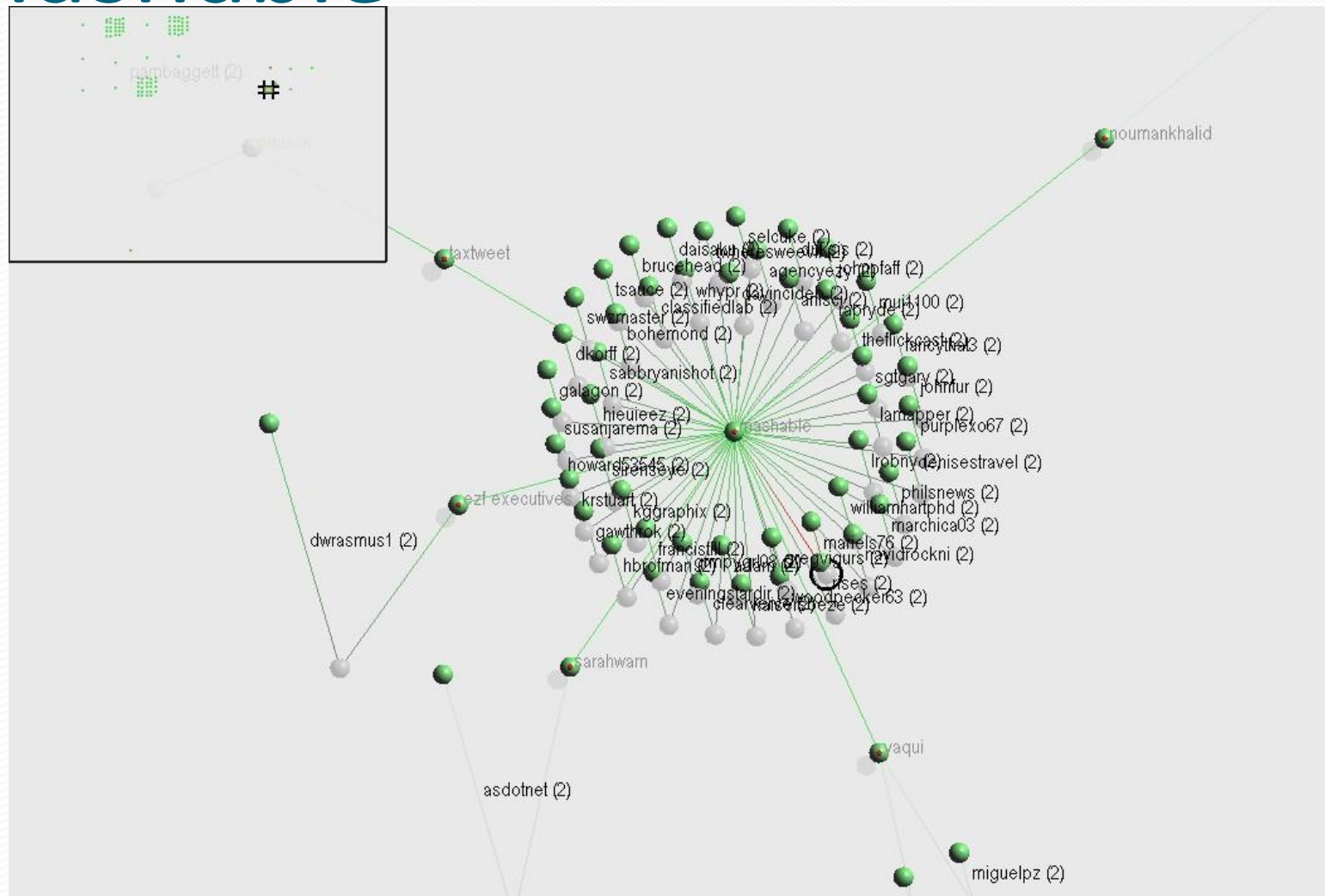


Acorn





mashable



The Short-Term Goal

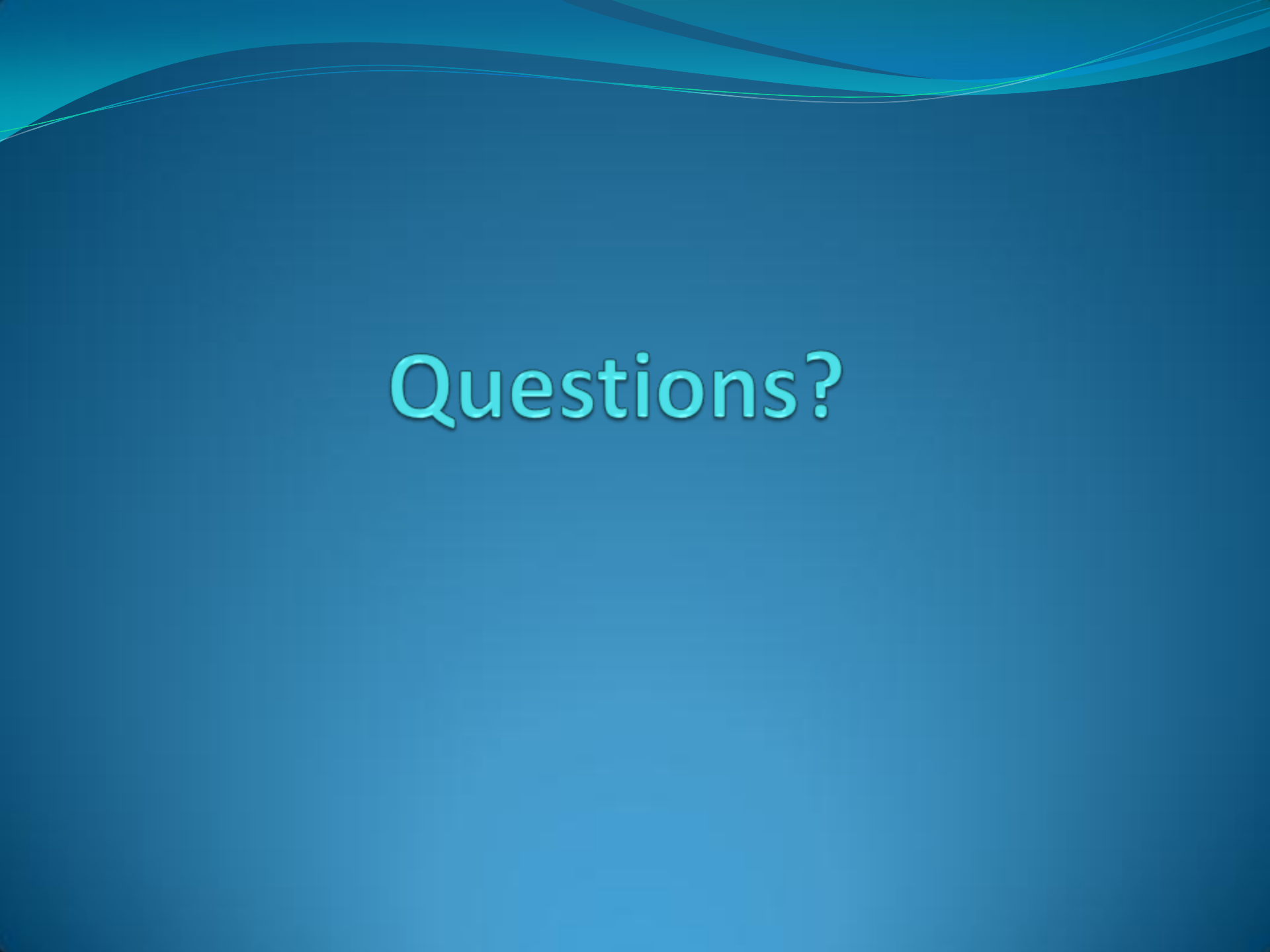
- While some networks are exactly as one would expect, sometimes a user finds anomalies. There are situations in which the user's experience suggests that the graph does not accurately reflect the actual patterns.
- We would like the user to be able to look at a particular graph. When the user finds a group of nodes that should be connected but are not, the user should be able to select those nodes and create a cluster.

Initial Steps

- We will be using an API to obtain Twitter data.
- We will create a client-server architecture in which the output of the graph visualization software will be modified by the server side program before being sent back to the client.
- We may also create a plugin for the software which will create and keep track of the clusters.

References

- M. Thottan and C. Ji, Anomaly Detection in IP Networks, IEEE Transactions on Signal Processing, Vol. 51, No. 8, August 2003.
- J. Abello, F. van Ham and N. Krishnan, ASK-GraphView: A Large Scale Graph Visualization System, IEEE Transactions on Visualization and Computer Graphics, Vol. 12, No. 5, September/October 2006.
- Graphs were created using ASK-GraphView using Twitter data.



Questions?