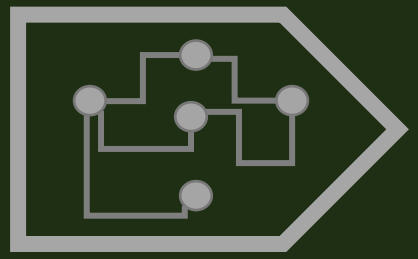


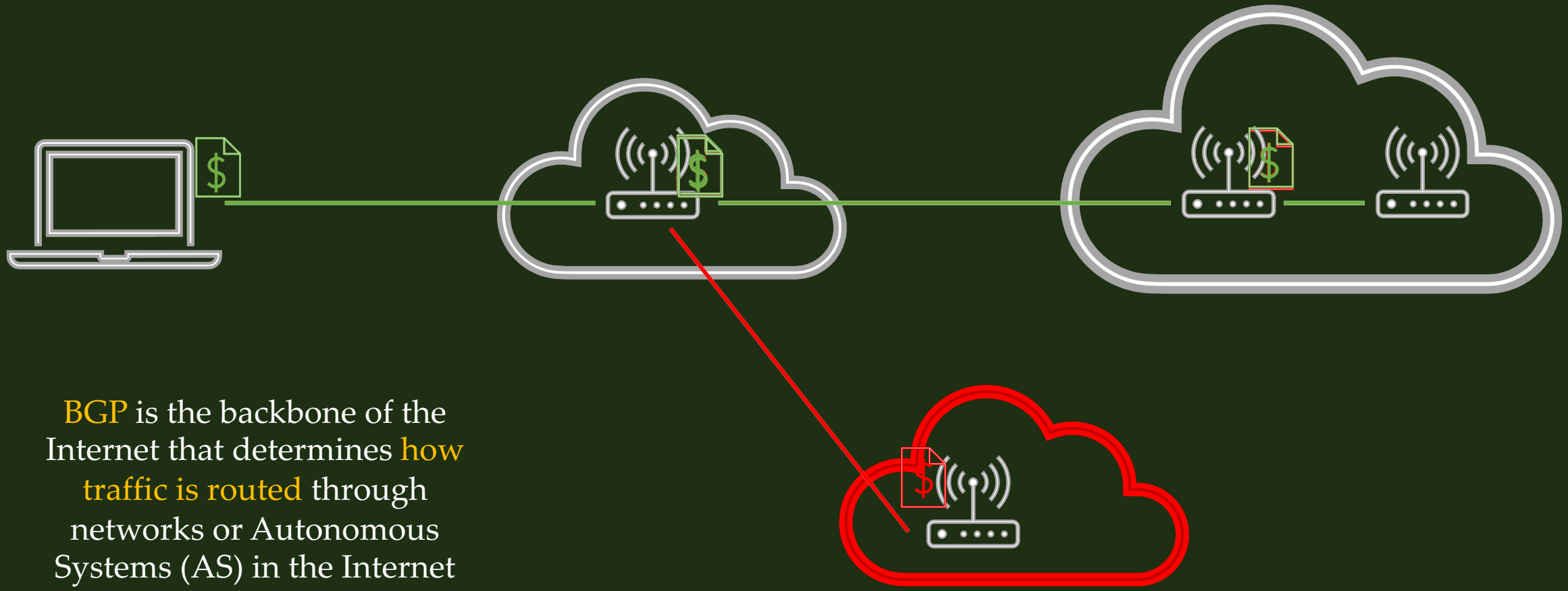
Modelling Border Gateway Protocol (BGP) for Anomaly Updates using Machine Learning

Janel Huang

Supervisors: Winston Seah and Marcus Frean

Mentor: Murugaraj Odiathevar

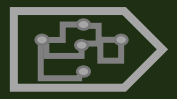
Introduction



BGP is the backbone of the Internet that determines how traffic is routed through networks or Autonomous Systems (AS) in the Internet

Problem

- Current methods of historical BGP, time series, and reachability check cannot automatically learn from experience
- Applying machine learning methods to find complex patterns in data that humans cannot discover
- Node level features used to detect anomalies
  - Average Autonomous System (AS) path length
  - Number of withdrawals or announcements
- No consideration on the entire network graph
- Incapable of real-time detection and determining the source of the anomaly
- Need to select network-level features to detect anomalies



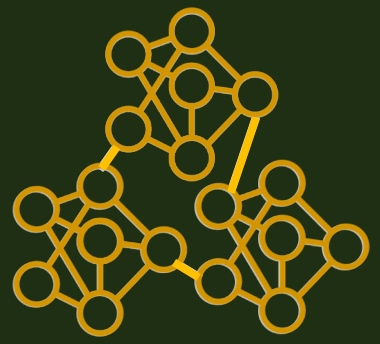
Proposed Solution

BGP Updates

Graph

Machine Learning

Features Extracted



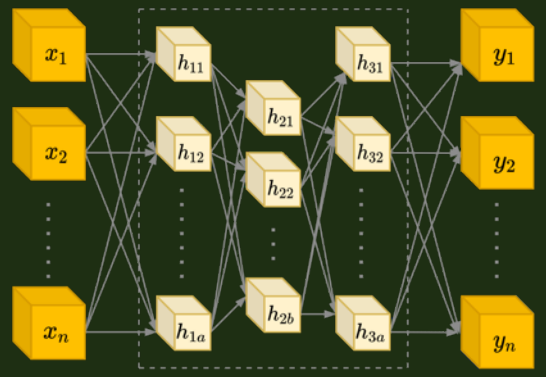
Closeness Centrality

Degree Centrality

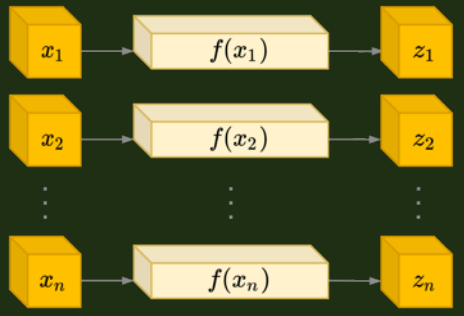
Eigenvector and betweenness centralities not feasible in memory and time

Interconnectivity or clustering coefficients of the entire network lose individual network information

Machine Learning Algorithms



Autoencoders



Univariate Gaussian(UG)

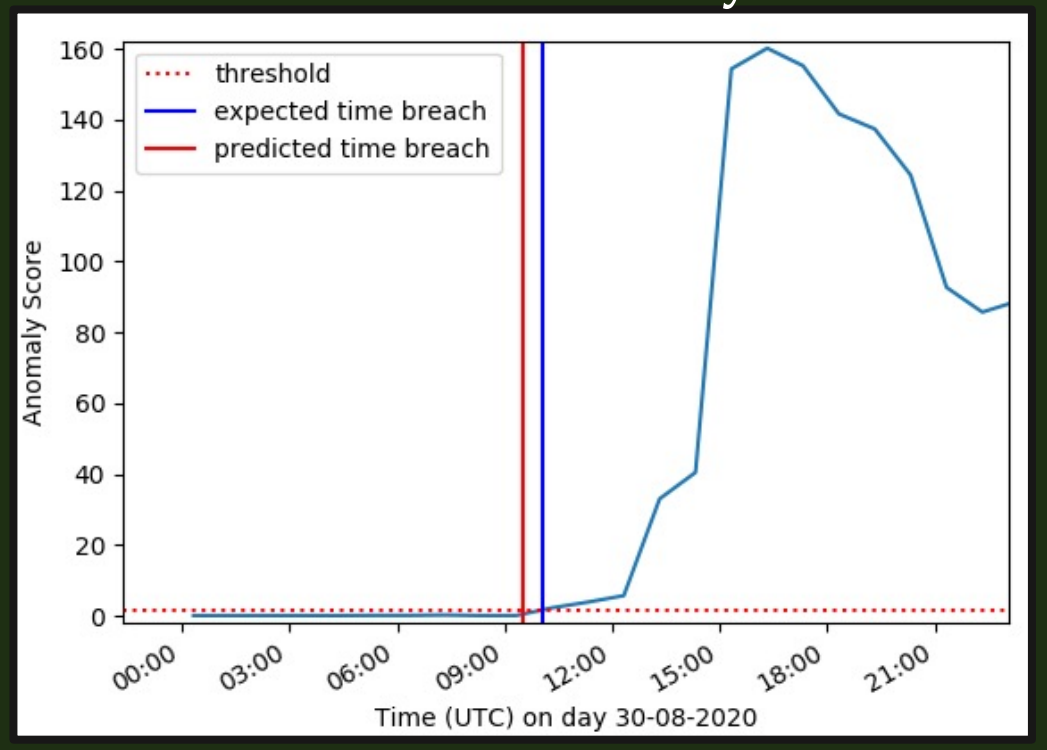
Entire anomaly detection using Autoencoders and UG and individual anomaly detection using UG

UG is instable in detecting anomalies from routers that have a limited visibility

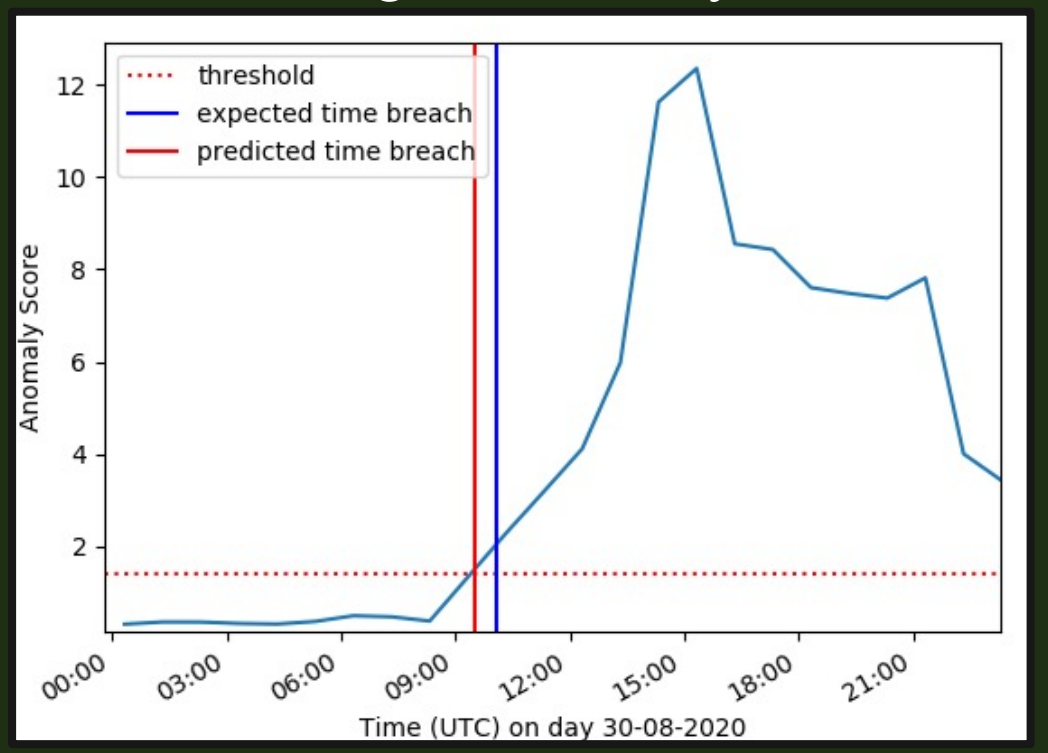
Experimental Results

Entire Network

Closeness Centrality

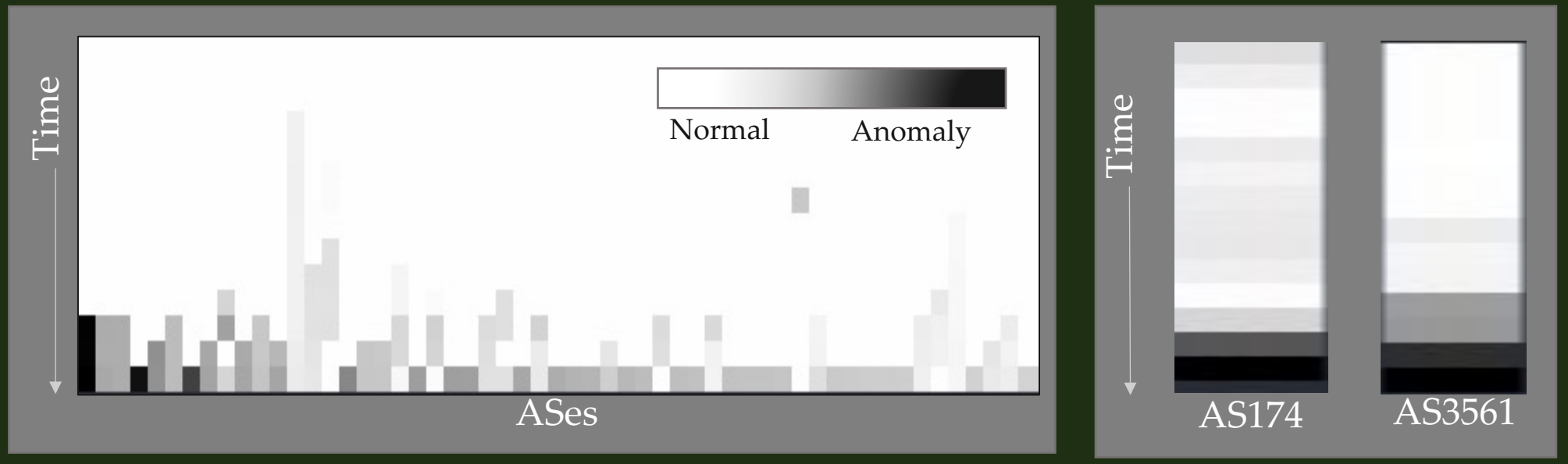


Degree Centrality



Closeness and degree centrality was able to detect the anomaly in the entire network earlier

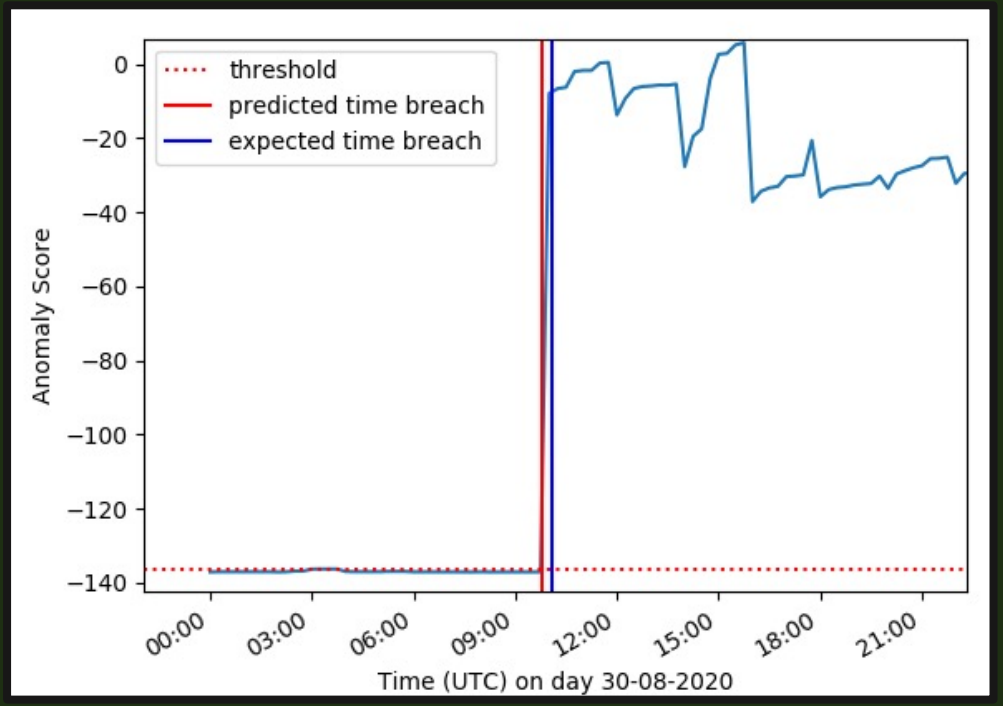
Entire Network: Visualisation



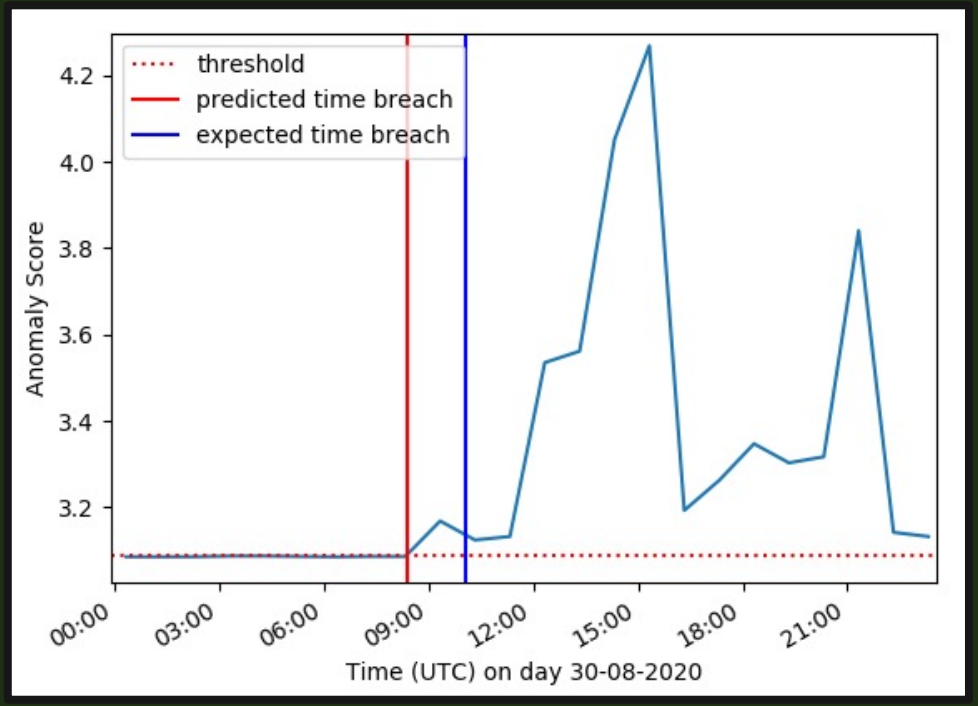
Severity Level of BGP incidents can be determined through the number of networks affected

Individual Networks

AS38022 (REANNZ)



AS3561 (CenturyLink)



Source of the anomaly can be determined using the time at which the anomaly threshold is breached

Conclusion

Anomaly Detection for the Entire Network And Individual Networks

Source of BGP incident

Contributions

- Use of graph-level features to determine anomalies
- Reporting the severity of the incident using a black and white image of the number of ASes affected
- Corroborating of multiple networks such as New Zealand, Japan and Serbia to determine anomalies

Questions