Department of Computer Science, University of British Columbia

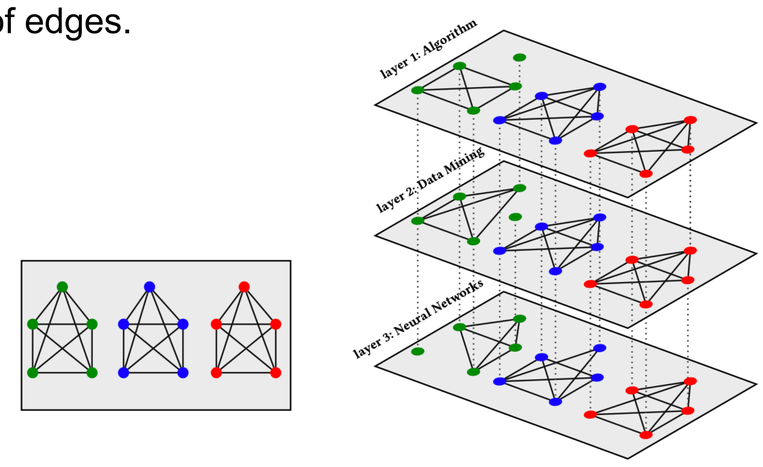
Anomaly Detection in Complex Networks

Ali Behrouz, Sadaf Sadeghian, Margo Seltzer

Problem

How do you detect anomalies in graphs with different types of edges?

Multiplex Networks:
Multiplex networks are graphs with different types of edges.



(a) Single-layer perspective (b) Multiplex perspective

Applications

Abnormal activity detection in the human brain:
- A fundamental task in neuroscience.
- Detecting brain disease or disorders.

- **Brain Networks:**
  Nodes: regions of interest (ROIs),
  Edges: high functional correlations between ROIs.

Fraud Detection in Multiple Blockchains:
- Cryptocurrency criminals make cross-cryptocurrency trades to hide their identity.
- Detecting suspicious transactions and identifying criminal activities across several blockchain transaction networks.

Challenges

1. Anomalies are **complex** and do **not** follow a **single pattern**.
2. **Interactions** between objects are complex and of **different types**.
3. The **importance** of each relation-type can varies among objects.
4. Object characteristics **change** over time.
5. **Lack** of high-quality **labeled data** for training.

ANOMULY is **the first edge anomaly detection** framework for **multiplex dynamic networks.**

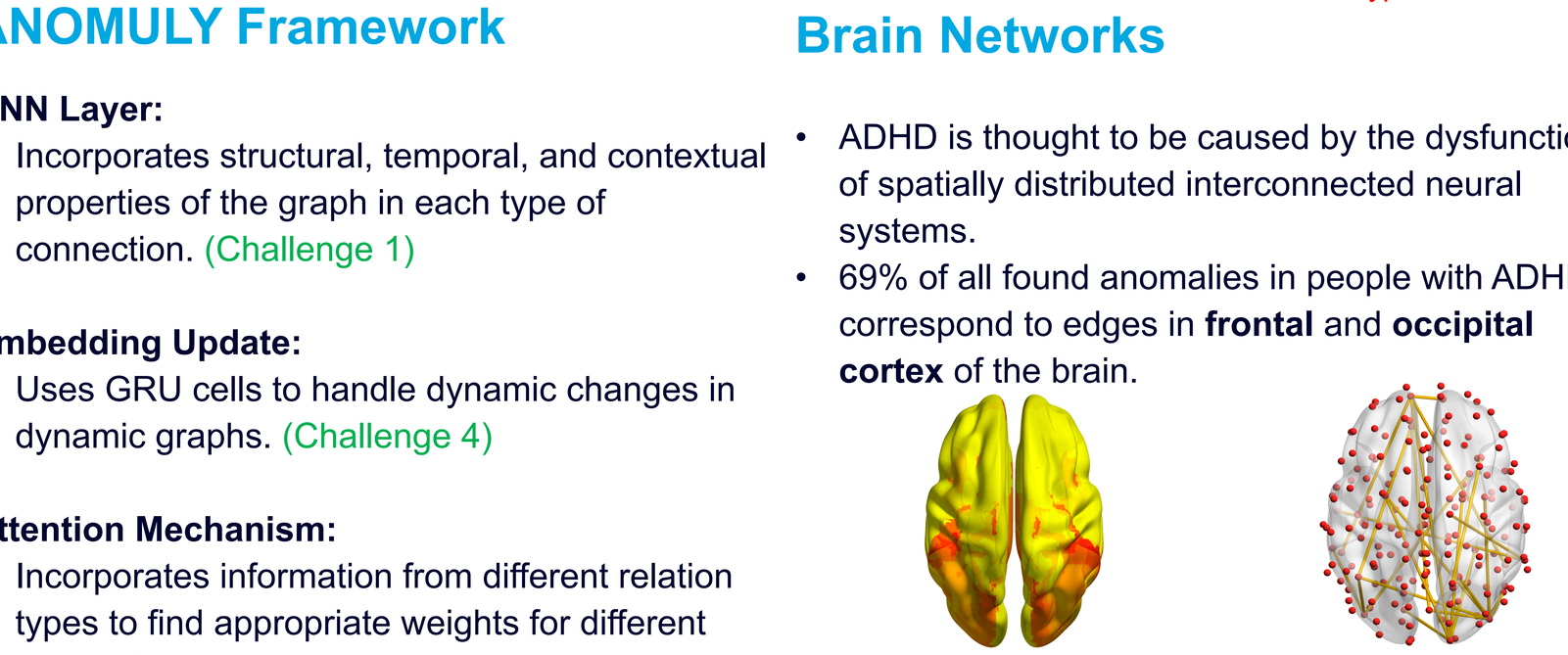


Figure 1. Framework and design of ANOMULY model

ANOMULY Framework

GNN Layer:
- Incorporates structural, temporal, and contextual properties of the graph in each type of connection. (Challenge 1)

Embedding Update:
- Uses GRU cells to handle dynamic changes in dynamic graphs. (Challenge 4)

Attention Mechanism:
- Incorporates information from different relation types to find appropriate weights for different types of connections. (Challenge 3)

Negative Sampling:
- Uses negative samples to train the model in an unsupervised manner. (Challenge 5)

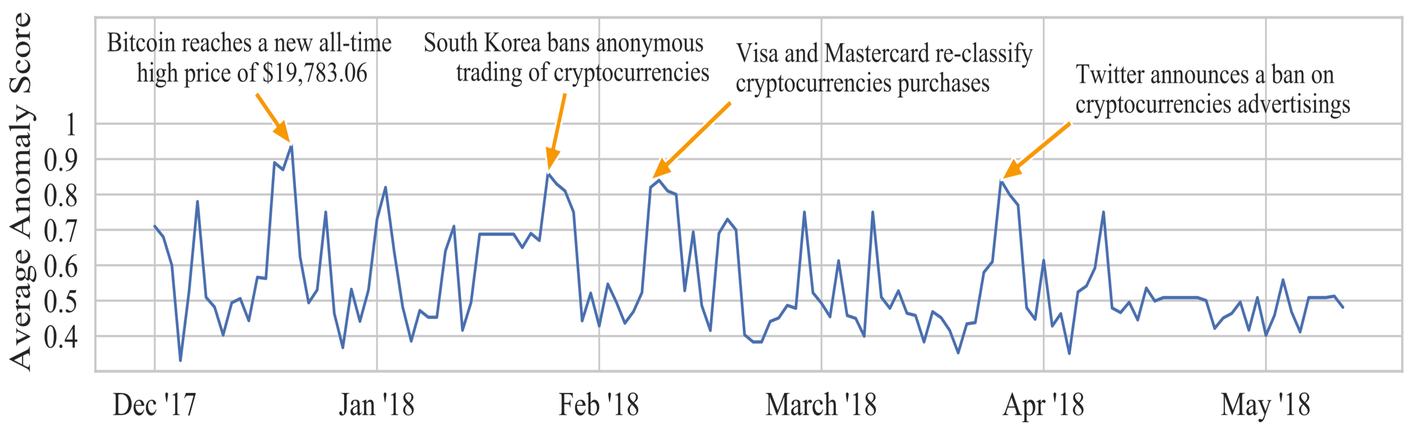
Detection Rate

Datasets: 9 datasets from social, co-authorship, blockchain, and co-purchasing networks domains.

- **Single-layer Networks:** ANOMULY outperforms single-layer methods by **5.94% to 9.98%**.
- **Multiplex Networks:** ANOMULY outperforms multiplex methods by **8% to 17.36%**.

Event Detection

- The top-4 local maximums all coincide with **major events** annotated in the figure.



Paper

Brain Networks

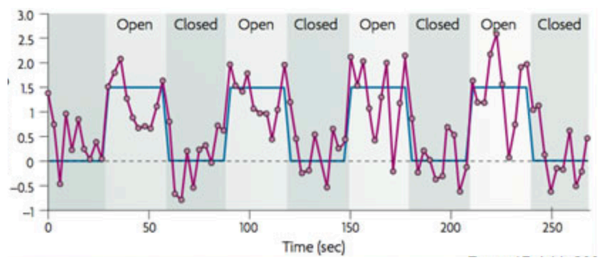
- ADHD is thought to be caused by the dysfunction of spatially distributed interconnected neural systems.
- 69% of all found anomalies in people with ADHD correspond to edges in **frontal** and **occipital cortex** of the brain.

(a) Distribution of anomalous edges

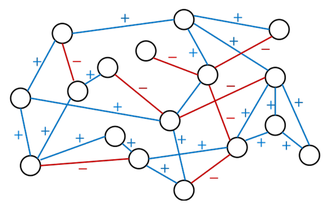
(b) Anomalous edges

Future Work

- **Task-based fMRI:** resting fMRIs cannot fully take advantage of temporal properties.
  In Task-based fMRI, each activity can be viewed as a snapshot of a temporal network.



- **Signed Network Anomaly Detection:**
  Relationships between two nodes can be positive or negative.
  E.g., blockchain, social media, and brain networks.



- **Hypergraphs Anomaly Detection:** Hyperedges can connect more than two nodes, capturing more complex relationships.
  E.g., Authors of a paper, users buying the same products, higher-order correlations in the brain.