GraphGuard

Tarek Solamy, Mohammad Asir, Armen Nanayan

Advisor: Professor Maminur Islam

Affiliation: Department of Computer Science, Trinity College

Introduction

GraphGuard is a diffusion-based model for detecting and mitigating anomalies in dynamic graphs, trained on data simulating network attacks.

Significance

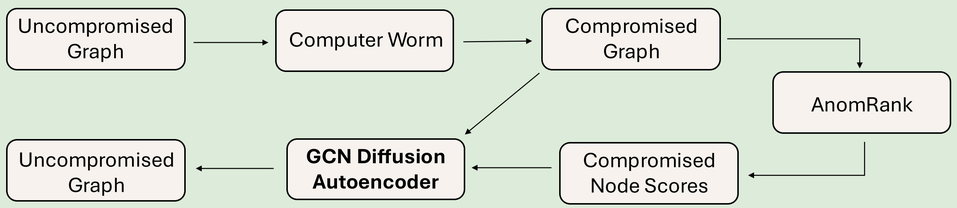
This project integrates a **diffusion-based model** with **AnomRank** to enable real-time **anomaly detection** and **threat mitigation** in dynamic graphs. By simulating how attacks propagate and affect graph structure over time, it strengthens the resilience of critical network systems. The goal is to build a responsive, graph-aware model capable of early detection, protection, and adaptive recovery from evolving cyber threats.

Technologies and Models

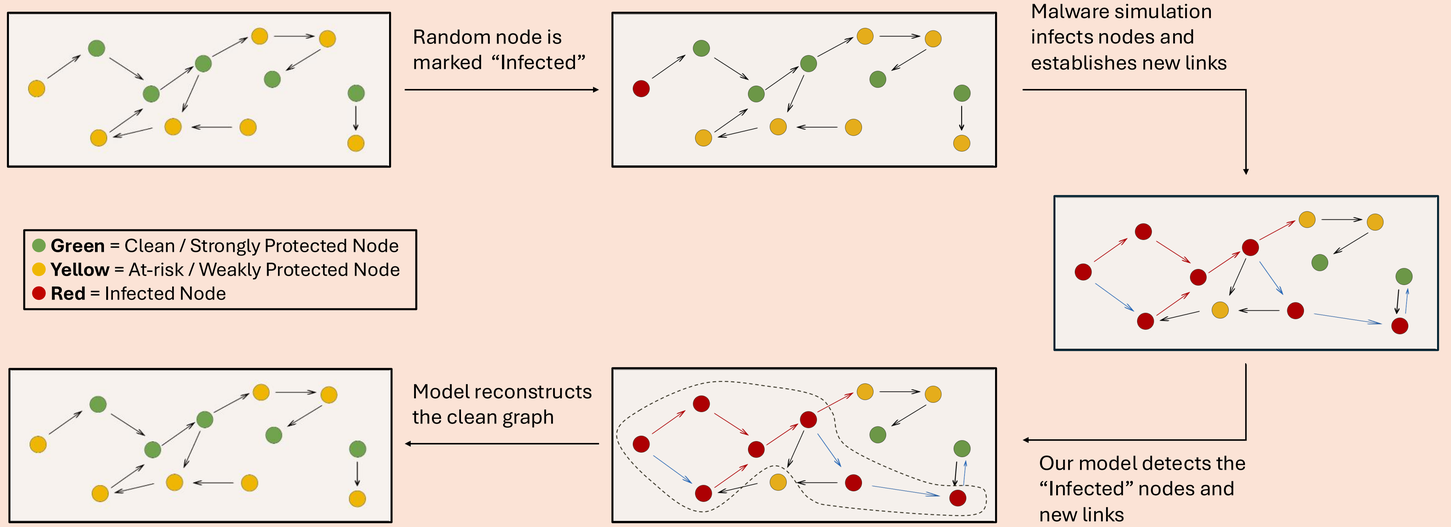
GraphMaker

AnomRank

Model Design



Mechanics of the Model



Model Training

Loss Function

Structural

"Rebuilding the Network's Blueprint"

Graph-Theoretic

"Preserving Hidden Patterns"

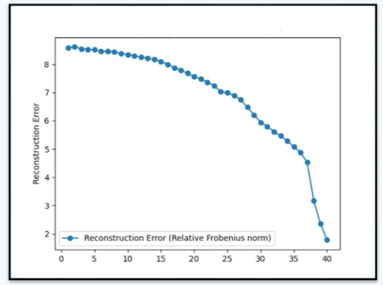
Latent Space Regularization

"Keeping the model's predictions consistent"

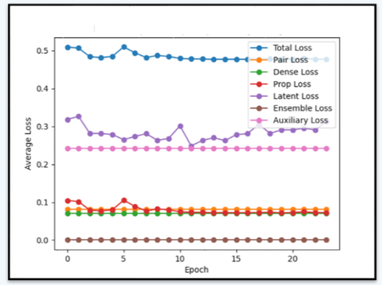
Auxiliary

"Training the inner detective"

Results



Reconstruction Error over Batch Size



Loss Components per Epoch for 91's Simulation

Future Work

- **Broaden Infection Types:** Extend the model to include diverse malware.
- **Publish Research:** Prepare a paper to share our results.
- **Improve Prediction:** Enhance the model to forecast malware spread and isolate threats early.