REAL TIME ANOMALLY DETECTION ON IOT USING GNN

TEACHER HARMANJOT KAUR

INTRODUCTION!

The **Internet of Things (IoT)** is transforming industries by connecting billions of devices that communicate and exchange data autonomously. However, this connectivity exposes IoT systems to various security threats such as device hijacking, data leakage, and unauthorized access. Detecting anomalies (unusual or malicious activities) in real-time has become critical for ensuring the security and reliability of IoT networks.

OBJECTIVE…

The main objective of this project is to develop and implement a **real-time anomaly detection system** for IoT networks using **GNN-based learning**.
The specific goals include:

- Modeling IoT devices and their interactions as a **graph structure**.
- Using **Graph Convolutional Networks (GCN)** to detect anomalous devices or communication patterns.
- Visualizing the IoT network and highlighting anomalies in real time.
- Demonstrating the effectiveness of GNNs in cybersecurity applications.

PROPOSED SYSTEM

Nodes represent IoT devices.

Edges represent communication or data flow between devices.

Features describe each device's behavior or operational state.

METHODOLOGY…

- **Step 1 – Data Representation**
  - Randomly generate `num_nodes` representing IoT devices.
  - Assign `num_features` to each node, representing metrics such as CPU usage, latency, or packet rates.
  - Create random communication links (`edges`) between nodes to simulate a network topology.
  - **Step 2 – Labeling**
  - Assign binary labels:
    - `0` → Normal device
    - `1` → Anomalous device (randomly selected)
    - **Step 3 – Graph Creation**
  - The data is stored in a PyTorch Geometric `Data` object containing node features, edges, and labels.

- **Step 4 – Model Architecture**
- The **GCN** model includes two convolutional layers:
  - **Conv1:** Extracts hidden node representations by aggregating neighbor features.
  - **Conv2:** Outputs class probabilities for normal and anomaly labels.
- The ReLU activation function introduces non-linearity, and the model is optimized using the **Adam optimizer** with a learning rate of 0.01.
- **Step 5 – Training**
- The model runs for 100 epochs, minimizing **cross-entropy loss** to improve classification accuracy.
- Loss is printed every 10 epochs to monitor convergence.
- **Step 6 – Inference and Visualization**
- Once trained, the model predicts each node's class label.
- Using **NetworkX** and **Matplotlib**, the IoT graph is visualized:
  - **Red nodes** represent anomalies.
  - **Green nodes** represent normal devices.

TOOLS AND TECHNOLOGIES

Programming Language: Python

Frameworks & Libraries:

PyTorch — Deep learning framework

PyTorch Geometric — For graph-based neural networks

NetworkX — For graph modeling

Matplotlib — For visualization

NumPy — For numerical operations

EXPECTED OUTCOME…

- A **graph-based machine learning model** capable of detecting anomalies in IoT networks.
- A **visual representation** of the IoT network where anomalies are clearly marked.
- **Real-time adaptability**, allowing the model to identify irregular behavior as data evolves.

APPLICATIONS

- **Smart Cities:** Detecting faulty or compromised sensors.
- **Industrial IoT:** Identifying abnormal machinery or communication patterns.
- **Healthcare IoT:** Monitoring connected medical devices for unauthorized activities.
- **Home Automation:** Detecting compromised smart devices (like cameras or speakers).

ADVANTAGES

- Learns **both feature-based and structural patterns**, improving detection accuracy.
- Reduces false positives compared to traditional methods.
- Scalable for large IoT environments.
- Provides interpretable graph-based insights for network administrators.

CONCLUSION

THIS PROJECT DEMONSTRATES THE USE OF **GRAPH NEURAL NETWORKS (GNN)**, PARTICULARLY **GRAPH CONVOLUTIONAL NETWORKS (GCN)**, FOR REAL-TIME ANOMALY DETECTION IN IOT NETWORKS. BY REPRESENTING IOT SYSTEMS AS GRAPHS, THE MODEL EFFECTIVELY LEARNS COMPLEX RELATIONSHIPS BETWEEN DEVICES AND IDENTIFIES ABNORMAL NODES WITH HIGH ACCURACY. THIS APPROACH CAN SIGNIFICANTLY ENHANCE IOT SECURITY, PAVING THE WAY FOR INTELLIGENT, SELF-MONITORING IOT SYSTEMS.

Project By

Name: Sanjay Bodh,Shivam
Institution: Chandigarh University
Department: Computer Application