The Iby and Aladar Fleischman
Faculty of Engineering
Tel Aviv University

Project Number : 22-1-239
By : Daniel Wolkowicz
& Shiraz Israeli

# Anomaly Detection In Communication Networks

## INTRODUCTION & MOTIVATION

In this project we implemented an automated system to efficiently detect anomalies in Communication Networks.

This project is motivated by the necessity to identify anomalies in communication networks, crucial for the daily operations of vital industry organizations. With numerous potential risks in network disruptions and cyberattacks, timely anomaly identification and efficient network management are necessary.

Using well-established machine learning techniques and historical data collection,
we classify anomalies, such as network-clogging broadcast packets.
The system improves network management, and can help identifying issues early on.

## WORKFLOW

1

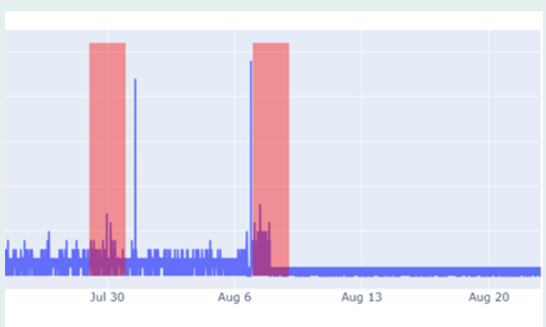
**Data Collection :**
Creating an interface using Ansible - Playbooks to collect data and create the database with the relevant features (connecting to the University network switches)

2

**Data Research :**
Examination of the data through visualization and statistical tools to discover patterns and trends and to get a comprehensive understanding of each interface characteristics.
This step also includes data pre-processing.

3

**Models :**
Testing diverse algorithms to classify anomalies for unsupervised data.
Using the "Rolling Windows" method, helping algorithms in identifying anomalies within specific time windows



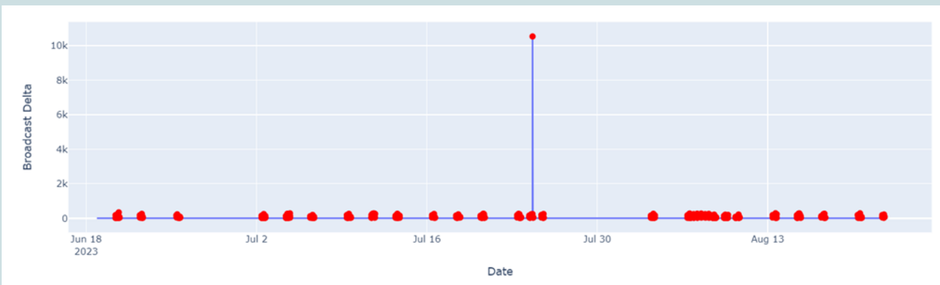

4

**Evaluation :**
Analyzing results and algorithm performance, to determine the optimal model, and presenting the chosen algorithm.
Improving the algorithm and its ability to distinguish "broadcast" anomalies.


## RESULTS

After testing a few algorithms,
and after analyzing the results for each model, we chose to implement the **"IsolationForest "** algorithm for our system.

Here's an example for an anomaly detection for one of the interfaces :




## FUTURE WORK

- Detecting suspicious points over time :
The system identifies non-usual broadcasts occurring simultaneously on multiple interfaces over time, suggesting investigations when anomalies arise.

- Improve our algorithm can be made by using the rest of the features that have been collected into our data base in the first step of our project.