Anomaly Detection in Communication Networks using ML

Project Team Member: Gowri V S , Sumedha J S, Srilikhita Balla , Mukesh Vanika

Supervisor Name: Dr. Abhay Gandhi

Department of Electronics and Communication Engineering

Visvesvaraya National Institute of Technology, Nagpur-INDIA

Problem Formulation

- Communication networks are susceptible to different attacks. So, there is a need of an efficient and intelligent system to protection networks from the attacks.
- Traditional rule based IDSs are not useful for more advanced times where anomaly and intrusion pattern change
- Thus the need for machine learning and deep learning based systems arise

Motivation

- In order to cater to the college network, we formulated the problem based on the most frequently faced issue of network attacks and come up with a efficient Machine learning based algorithm, which detects and categorize various types of anomalies and intrusions.

Introduction

Types of intrusion detection mechanisms include Misuse detection(signature-based) and anomaly detection(behaviour-based)

Misuse based methods are highly effective to detect known attacks. Anomaly detection methods use the normal system activity to detect anomalies that deviate from these.

Types of anomalies include : Point anomalies, contextual anomalies, collective anomalies

Different types of attacks include - DoS attack (flooding/crashing services), DDoS attack etc.

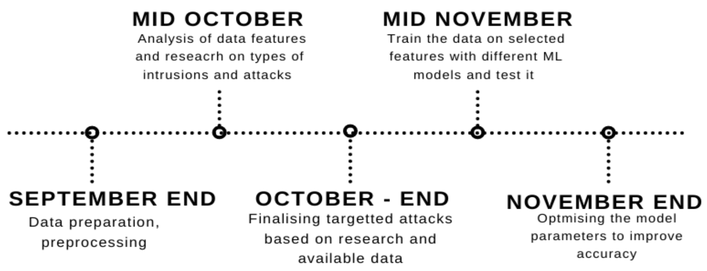
References

1. A. L. G. Rios, Z. Li, K. Bekshentayeva and L. Trajković, "Detection of Denial of Service Attacks in Communication Networks," 2020 IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1-5, doi: 10.1109/ISCAS45731.2020.9180445.
2. Ismail et al., "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," in IEEE Access, vol. 10, pp. 21443-21454, 2022, doi: 10.1109/ACCESS.2022.3152577.
3. Bonte, Pieter Hautte, Sander Lejon, Annelies Ledoux, Veerle De Turck, Filip Hoecke, Sofie Ongenae, Femke. (2020). Unsupervised Anomaly Detection for Communication Networks: An Autoencoder Approach. 10.1007/978-3-030-66770-212.
4. Kumari, Kimmi, and M. Mrunalini. “Detecting Denial of Service Attacks Using Machine Learning Algorithms - Journal of Big Data.” SpringerOpen, 28 Apr. 2022,

Literature survey

- – Using packet size and inter-arrival time of requests, we compute threshold.
  – Using the computed throughputs, we calculate the threshold using median.
  – Using Naive-Bayes and Logistic Regression, we check if throughput is above the threshold. If it is, it is categorized as an attack.
- – Based on the number of packets requested, we can classify anomalies into four types- outliers, trend changes, variance changes and level shifts.
  – Various Architectures such as Dense AE, LSTM AE, LSTM seq2seq, TCN AE and TCN seq2seq was implemented to classify these anomalies.
  – It was observed that TCN seq2seq architectures perform best on the artificial datasets ,while dense AE shows best results on the real use case data.

TimeLine



Methodology

Steps to proceed with the project :

1. Data collection : Train the data using data collected from packet sniffing tools (eg - Wireshark).
2. Simulation of common attacks and anomalies into the network using software tools (eg - NPing used to simulate ping flood common in DoS attacks)
3. Pre process the data and analyse the features :
   (a) Source and destination ip address
   (b) Type of protocol
   (c) Time taken for request completion
   (d) Packet length
   (e) Other information (whether retransmission was initiated, duplicate acknowledgement of request etc)
4. Train the model on the dataset and check efficiency and accuracy of different models
5. Finally test the dataset for the college network dataset to obtain the accuracy

Results

Formulated the problem statement after researching on the need to have an efficient learning based system to detect anomalies

Researched on the existing methods for anomaly detection and need for machine learning based algorithms

Researched the different types of attacks possible in the communication network and also on the importance of this project specifically to the college network

Conclusion

1. The numerous variety of attacks make it a necessity to have an intelligent learning based algorithm to detect the attacks
2. Firewalls and other current IDS use statistical methods to detect anomalies and intrusions
3. Need to find the best parameters/features to train the model on to get best accuracy